Aberdeen AberNAS LX Series

Setup and Administration Guide

Publication Date: June 2009

CUSTOMER SUPPORT INFORMATION
Mailing address: **Aberdeen LLC** 9130 Norwalk Boulevard Santa Fe Springs, CA 90670
Phone (562) 699-6998 Sales (800) 552-6868 Fax (562) 695-5570
Web site: **www.aberdeeninc.com** E-mail: **CustomerService@aberdeeninc.com**

ABERDEEN LLC END USER LICENSE AGREEMENT

This End User License Agreement (“Agreement”) is a legal agreement between Aberdeen LLC (“NE”) and you (“Licensee”) the subject matter of which is NE’s Network Attached Storage or Net work Storage Solution products and any applicable updates or upgrades thereto (“Product”) and which may include associated media and printed or electronic (retrievable via computer net works such as the Internet or otherwise) materials (“Documentation”) (collectively referred to herein as “Product”). By breaking any seal on the Product, installing, copying or otherwise using the Product (“Licensee’s Acceptance”) Licensee agrees to be bound by the terms and conditions of this Agreement. If Licensee does not agree to the terms and conditions of this Agreement, Licensee must not install copy or otherwise use the Product and shall promptly return the Product to the place of purchase for a refund of the purchase price, if any. 1. Grant of License. Subject to the terms and conditions of this Agreement and Licensee’s acceptance thereof, NE hereby grants to Licensee and Licensee hereby accepts a personal, non-transferable, nonexclusive license (which shall be revocable pursuant to the terms of this Agreement) to use the Product according to its merchantable purpose and pursuant to the terms and conditions of this Agreement. 2. Network License. Licensee may provide access to the Product for its employees and other applicable users, subject to each of such users understanding and complying with the terms and conditions of this Agreement. Licensee may not, nor any of it’s employees nor other applicable users, make a copy of the operating system and its related software applicable to the Product. 3. Limitations and Restrictions. Except as expressly permitted herein, Licensee may not: (i) copy, alter, adapt, modify, translate, or create derivative works of the Product or any portion thereof; (ii) reverse engineer, decompile, disassemble, or at tempt to derive the source code of the Product or any portion thereof, unless and only to the extent any of the foregoing is expressly permitted by applicable law and may not be restricted there under; (iii) separate the Product into component parts for transfer to or use by a third party; (iv) rent, lease, loan, sell, distribute, sublicense or lend the Product; (v) remove, alter or obscure any proprietary notices; or (vi) otherwise use the Product. 4. Reservation of Rights. NE does not grant and Licensee does not obtain any implied licenses under this Agreement. NE reserves all rights, title and interests of any kind that are not expressly granted to Licensee in this Agreement. 5. Intellectual Property Rights. NE retains title to and all ownership interests in all proprietary rights, including without limitation copyrights, trademark rights, patent rights, trade secret rights, and any other intellectual or industrial property rights throughout the world (“IPR”), with respect to the Product and all copies or portions thereof, whether or not incorporated into or used in connection with any other products, including without limitation soft ware or documentation materials. Licensee acknowledges that the Product is licensed and not sold under this Agreement, that nothing in this Agreement shall constitute or be construed to constitute a sale of the Product or any portion or copy thereof and that no title to or ownership interest in any rights, including without limitation IPR, with respect to the Product or any components thereof is transferred to Licensee. 6. DISCL AIMER OF WARR ANT Y. THE PRODUCT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY OF ANY KIND. NE MAKES NO REPRESENTATION OR WARR ANT Y OF ANY KIND, WHE THER E XPRESS OR IMPLIED (EITHER IN FACT OR BY OPER ATION OF L AW), WITH RESPECT TO OR REL ATING TO THE PRODUCT OR THIS AGREEMENT. NE EXPRESSLY DISCLAIMS ALL IMPLIED WARR ANTIES, INCLUDING, WITHOUT LIMITATION, ALL WARRANTIES OF ACCUR ACY, MERCHANTABILIT Y, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT AND ALL WARR ANTIES THAT MAY ARISE FROM COURSE OF DE ALING, COURSE OF PERFORMANCE OR USAGE OF TR ADE. NE DOES NOT WARR ANT THAT THE PRODUCT WILL BE ERROR-FREE OR THAT OPER ATION OF THE PRODUCT WILL BE UNINTERRUPTED, AND HEREBY DISCL AIMS ANY AND ALL LIABILIT Y ON ACCOUNT THEREOF. NE MAKES NO WARR ANT Y THAT ALL ERRORS, FAILURES OR DEFECTS WILL BE CORRECTED. THIS SECTION 6 SHALL BE ENFORCE ABLE TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE L AW. Some jurisdictions prohibit the exclusion of implied warranties or limitations on how long an implied warrant y may last, so the above limitations may not apply fully to Licensee. In this case Licensee’s sole and exclusive remedy for a breach of warrant y shall be, at NE’s option and in its sole discretion, replacement or repair of the Product or return thereof for a refund of the purchase price, if any. Such remedy shall be available to Licensee for one (1) year commencing on the date of Licensee’s Acceptance and ending on the first anniversary thereof. 7. LIMITATIONS OF LIABILIT Y. IN NO E VENT SHALL NE, ITS AFFILIATES OR SUPPLIERS BE LIABLE TO LICENSEE, ITS AFFILIATES OR CUSTOMERS FOR ANY INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL OR PUNITIVE DAMAGESWHATSOEVER, INCLUDING WITHOUT LIMITATION DAMAGES FOR LOST PROFITS OR

RE VENUE, LOST BUSINESS OPPORTUNITIES, LOST OR INACCESSIBLE DATA OR INFORMATION, UNAUTHORIZED ACCESS TO DATA OR INFORMATION OR OTHER PECUNIARY LOSS, ARISING OUT OF OR REL ATED TO THIS AGREEMENT, THE SUBJECT MAT TER HEREOF OR THE AUTHORIZED OR UNAUTHORIZED USE OF OR INABILIT Y TO USE THE PRODUCT, WHETHER LIABILITY IS ASSERTED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE AND STRICT PRODUCT LIABILIT Y) OR OTHERWISE AND IRRESPECTIVE OF WHE THER NE HAS BEEN ADVISED OF THE POSSIBILIT Y OF ANY SUCH LOSS OR DAMAGE. IN NO EVENT SHALL NE'S AGGREGATE LIABILITY UNDER THIS AGREEMENT OR ARISING OUT OF OR RELATED TO THE SUBJECT MATTER HEREOF EXCEED ONE HUNDRED DOLLARS (US $100.00). Some jurisdictions do not allow the limitation of incidental or consequential damages so this limitation may not apply fully to Licensee, but such limitation shall apply to the maximum extent permitted by applicable law. Licensee acknowledges that the pricing of the Product and other terms and conditions of this Agreement reflect the allocation of risk set forth in this Agreement and that NE would not enter into this Agreement without these limitations on its liability. 8. Termination. This Agreement is effective until terminated. Without prejudice to any other rights or remedies NE may have at law or in equity, NE may immediately terminate this Agreement if Licensee fails to comply with any term or condition of this Agreement. Upon termination of this Agreement, Licensee shall immediately discontinue the use of the Product and at NE's option, return to NE and/or certify destruction of the Product and any related materials provided to Licensee by NE, and all full or partial copies thereof (whether in tangible or intangible form), in Licensee's possession or control. Licensee may also terminate this Agreement at any time by providing written notice to NE and certifying destruction of the Product and all full or partial copies thereof (whether in tangible or intangible form) in Licensee's possession or control. 9. General. With Licensee's Acceptance Licensee agrees to be bound by the terms and conditions set forth in this Agreement and Licensee acknowledges that it has read and understands this Agreement. Licensee further agrees that this Agreement is the complete and exclusive statement of the understanding between NE and Licensee which supersedes any proposal or prior agreement, oral or written, and any other communication between NE and Licensee relating to the subject matter of this Agreement. This Agreement may not be modified except in a writing duly signed by an authorized representative of NE and Licensee. If any provision of this Agreement is held to be unenforceable for any reason, the remaining provisions hereof shall be unaffected and shall remain in full force and effect. This Agreement shall be governed by and construed in accordance with the laws of the United States and the State of California as such laws are applied to contracts between California residents entered into and to be performed entirely within California. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement. Licensee hereby submits to the sole and exclusive jurisdiction of, and waives any venue objections against, the United States District Court for Northern California and the Superior Court of the State of California for the Count y of Santa Clara and the Santa Clara Municipal Court in regard to all disputes and litigation arising under or relating to this Agreement. Licensee's rights and obligations under this Agreement shall not be assignable, delegable, sub licensable or otherwise transferable, whether voluntarily, by operation of law or otherwise, without NE's prior writ ten approval except as provided herein. NE may freely assign this Agreement and/or its rights and obligations hereunder. Should you have any questions concerning this Agreement, or if you desire to contact NE for any reason, please visit: www.Aberdeeninc.com.com. 10. U.S. Government Restricted Rights. If Licensee is an agency or instrumentality of the United States Government, the soft ware and documentation associated with the Product are "commercial computer soft ware" and "commercial computer soft ware documentation", and pursuant to FAR 1 . 1 or DFARS 7.7 0 , and their successors, as applicable, use, reproduction and disclosure of the Product and its associated soft ware and documentation are governed by the terms of this Agreement. 11. Export Law Assurances. Licensee will not use or otherwise export or re-export the Product except as authorized by United States laws and regulations, including without limitation those of the U.S. Department of Commerce, and, as applicable, the laws and regulations of other jurisdictions.

Copyright © 2009 Aberdeen LLC All rights reserved.
AberNAS and ABERNAS are registered trademarks of Aberdeen.

- Contents -

Initial Setup: 8
- Connecting the AberNAS to your Network
- Locate the AberNAS using NASFINDER
- Assign Static IP or DHCP

Logging in to the AberNAS: 10
- Log-in to Command Line Using a Direct Console Connection
- Log-in with Command Line Using a SSH/Telnet Client

AberNAS LX Series Web Administration: 11
- Log-in to the Web Administration Graphical Interface

Web Administration Interface – Overview: 12

Server Configuration: General Settings: 13
- Edit General Settings
- Synchronize With A Custom NTP (Network Time Protocol)
- Server: Delete An Existing NTP (Network Time Protocol)
- Server: Provide NTP Synchronization Service To Attached
- Client: Provide NTP Synchronization Service To New Clients:

Server Configuration: Password Change: 15
- Change your root log-in password

Server Configuration: Restart & Shutdown: 16

Network Settings: TCP/IP Setting: 17
- Configuring TCP/IP to Gigabit Port(s)
- Remove A Port

Network Setting: Port Bonding: 19
- Bond Ports
- Remove Bond
- Bond Type Definitions

Network Settings: Microsoft Networking: 22

- Enable/Disable CIFS/SMB Service
- Join Microsoft Workgroup
- Join Microsoft Primary Domain Controller (PDC)
- Join Microsoft Active Directory Service (ADS)
- UNIX Networking
- Synchronize With Network Information Service (NIS)

Network Settings: Apple Networking: 25
- Allow Apple Clients To Access AberNAS Logical Volumes

Network Setting: LDAP Client: 26
- Configure LDAP Client Service

DHCP Service: 27
- Enable DHCP Service

FTP Service: 28
- Enable FTP Service

iSCSI Service: 29
- Enable The iSCSI Initiator Service
- Enable The iSCSI Target Service

Storage Management: Overview: 31
- Definitions for Volume Group Types
- Definition for RAID Volume Types

Storage Management: RAID Volume Manager: 33
- Managing RAID Volumes

Storage Management: Software RAID Manager: 34

Storage Management: External RAID Manager: 35

Storage Management: USB/1394 Volume: 36

Storage Management: iSCSI Initiator Management: 37
- iSCSI Target Device Benefits
- Discover Available iSCSI Target Portals And iSCSI Target Devices
- Connecting And Disconnecting iSCSI Target Devices
- PV/RV Information

Storage Management: Volume Group Manager: 39
- Creating PV
- Removing PV
- Adding RV To PV
- Separate The PV From Expanded PV
- Replace The PV In the Expanded PV With Another RV

Storage Management: Logical Volume Manager: 41
- Functions Of Logical Volume Manager
- Create A New Logical Volume
- Modify An Existing Logical Volume
- Delete A Logical Volume

Storage Management: Format: 44
- Format a Logical Volume

User & Access: Local User Management: 45
- Create Local Users
- Access a User's Home Directory
- Delete a User From The Local Users List
- Modify an Existing User

User & Access: Local User Group Management: 47
- Create Local User Groups
- Add User To User Groups
- Modify/Delete Local User Group
- Delete A User Group

User & Access: Access Control: Microsoft: 49
- Assign Access Control

- Host IP Blocking
- Add IP Address to Allow or Deny List
- Delete an IP Address to Allow or Deny List

User & Access: Access Control: UNIX: 51
- Add Host Access
- Delete The Host
- Security Method For NFS Access
- Mounting Syntax

User & Access: Access Control: Apple: 54
- Assign Access Control
- Restart AFP Service

User & Access: Access Control: iSCSI: 56
- Global and Target User(s)
- Creating A Global User
- Creating A Target User
- Delete User
- Host IP Blocking
- Add IP Address To Allow or Deny List
- Delete an IP Address To Allow or Deny List

User & Access: Quota Management: 59

Server Monitoring: Notification: 61
- Setup A Failure Notifications Procedure

Server Monitoring: Utilization: 63

Server Monitoring: General: 65

Server Monitoring: Server Log: 66
- View A Log Of Activities

Server Monitoring: User Access: 67

View Settings: General Settings: 68

View Settings: Network Settings: 69

View Settings: Storage Management: 71

View Settings: Access Control: 72

View Settings: Server Monitoring: 73

Back Up Mirror and Restore: 74

Snapshot and Restore: 74
- Create Snapshots
- Delete Snapshot
- Modify Snapshot

Backup Software Agent Install: 75

Server Fail-over and Mirror: 76
- Before Configuring SFM
- Configure SFM
- Re-deploy Failed Primary Server

Folder Replication: 79
- Add A Folder For Replication
- Enable Replication Scheduling

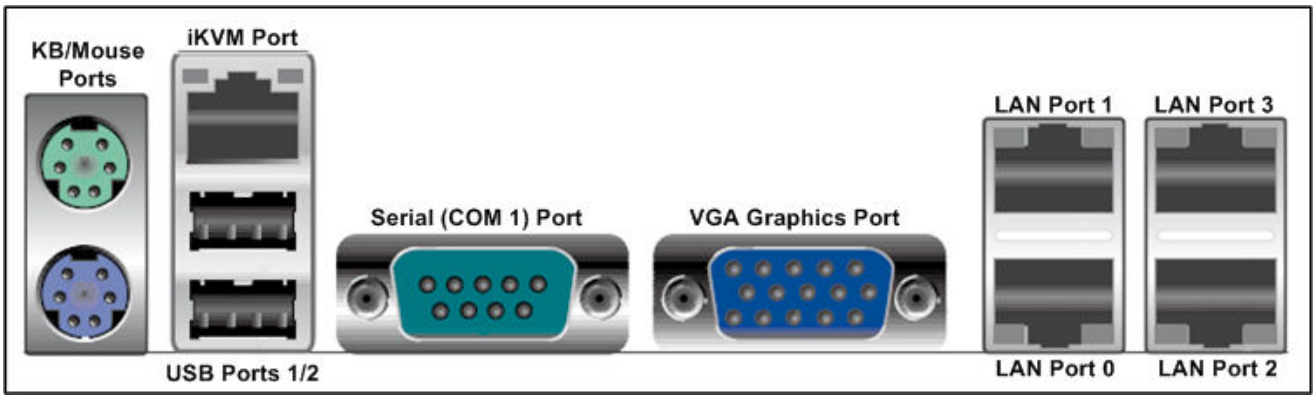
View Settings: Snap Shot and Restore: 82

AberNAS Update: 83
- AberNAS Update
- Updating The ABERNAS To The Latest Patch
- Reset The Server Setting To The Factory Defaults
- New License

Initial Setup – AberNAS LX Series

Connecting the AberNAS to Your Network

Connect the AberNAS to your network using a standard patch cable plugged into **Port 0** as shown below:



Locating the AberNAS using NASFINDER:

Insert the AberNAS setup CD into a computer that resides on the same network and run the **NASFINDER** setup utility. The NASFINDER.EXE utility is found in the following directory on the CD:

E:\Aberdeen_Manuals\AberNAS_Network_Attached_Storage\Linux_NAS_Software\NASDirector

Once located, run the NASFINDER setup utility.

If you are using Windows:

- Double click ***NASFINDER.exe*** in the **"NASDIRECTOR"** folder to start the setup.

If you are using Linux:

- Open a Terminal Session and *cd* to the **"NASDIRECTOR"** folder.
- Run application with ***./NASFinder*** command.

The Following screen will appear showing how many AberNAS units were found on your network:

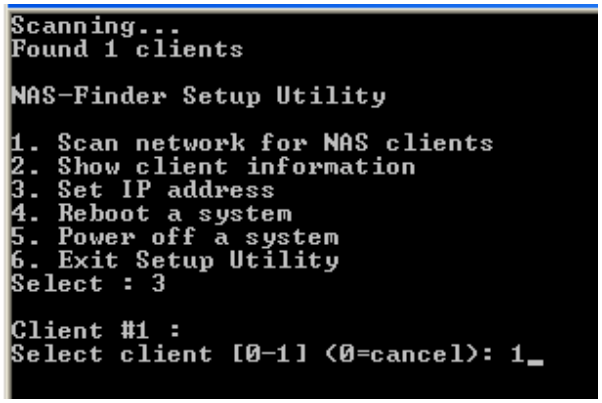
```
Scanning...
Found 1 clients

NAS-Finder Setup Utility

1. Scan network for NAS clients
2. Show client information
3. Set IP address
4. Reboot a system
5. Power off a system
6. Exit Setup Utility
Select : _
```

If you have more than one Linux AberNAS unit on your network, run option (**2**) to differentiate between them by IP address. Otherwise, proceed with option (**3**) to set the IP address.

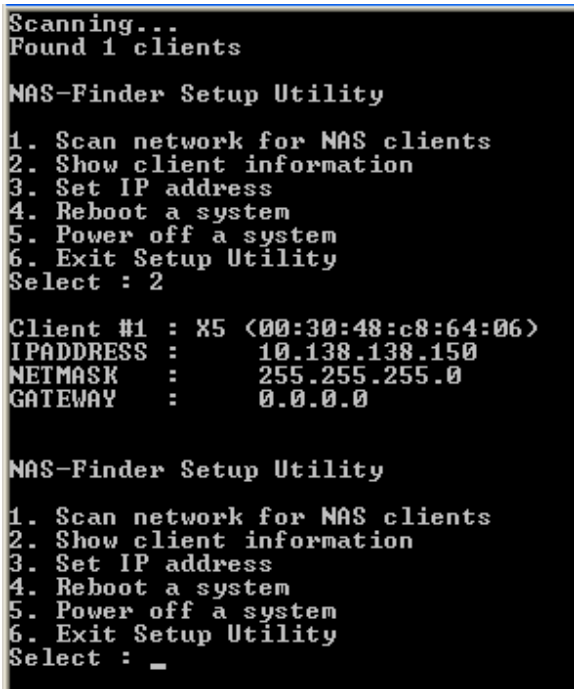
Press option (**3**) to set the IP address of the Linux AberNAS. You will be asked to select the Client #. Since only a single AberNAS should be found, select Client #1 and press <**ENTER**>



You will then be prompted for the password. Enter the default AberNAS password **0000** to proceed.

After you have entered the correct password, you will be prompted to select your preferred IP address type for the unit. Select (**1**) to enable DHCP, (**2**) to setup a static IP address or select (**0**) to cancel.

Most users will select option (**2**). You will be prompted to enter your preferred static IP address, Netmask and Gateway. Once completed you can verify that your preferred IP address has been properly set by choosing option (**2**) to show the client information as shown below:



Now the server must be rebooted by selecting option (**4**) for the settings to take effect.

From this point on, the AberNAS can be administered via its integrated web GUI by typing its IP address into your preferred web browser's address field.

Logging In to the AberNAS

Log-in to Command Line using a Direct Console Connection:

If for some reason you are unable to setup the AberNAS for the first time using the NASFINDER Setup Utility, you can also connect a keyboard and monitor directly to the AberNAS system and access the Linux command console.

At the log-in prompt, enter the following login credentials:

USER ID: **root**
PASSWORD: **0000**

Log-in to Command Line Using SSH:

Open an SSH on another computer and connect to the ABERNAS system by entering the appropriate commands:

For SSH, enter the following command using the ABERNAS system IP address in place of IP_Address:

ssh IP_Address (Example: **ssh 10.138.138.150**)

Note

The User ID and Password for SSH are the same as those used for the Direct Console Connection.

Log-in to Command Line Using Telnet:

For Telnet, enter the following command using the ABERNAS system IP address in place of IP_Address:

telnet IP_Address (Example: **telnet 10.138.138.150**)

At the log-in prompt, enter the following login credentials:

USER ID: **admin**
PASSWORD: **111111**

AberNAS LX Series Web Administration

Log-in to the Web Administration Graphical Interface:

Open a web browser on any computer that exists on the same network as the AberNAS and enter the IP address you assigned earlier into the address field as shown below. The AberNAS web GUI will appear.

Enter the default User ID and Password:

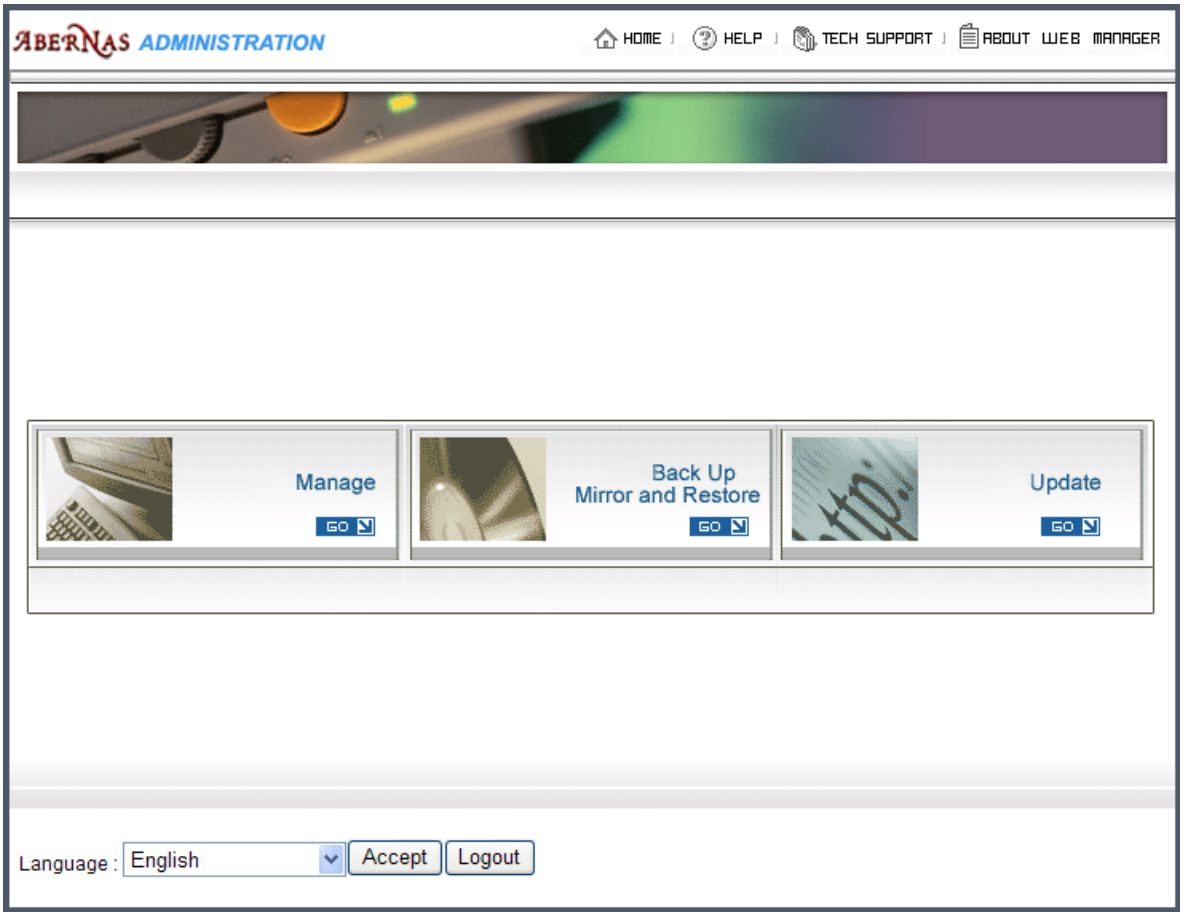
USER ID: root
PASSWORD: 0000

Click "**Enter**" to complete the AberNAS login process.

Web Administration Interface – Overview –

The ABERNAS offers a number of interfaces from which administrative tasks can be performed. This section describes how to navigate through the interface to access the administrative features.

The ABERNAS Administration Home (pictured below) is launched after successful log-in. The call outs indicate the functions and information that can be found behind each button:



Home – Link back to this screen from other administration screens or pages.

Help – Link to on-line product info and downloadable manual.

Tech Support – Link to on-line technical support information.

About Web Manager – Display version no. for OS build and installed patch.

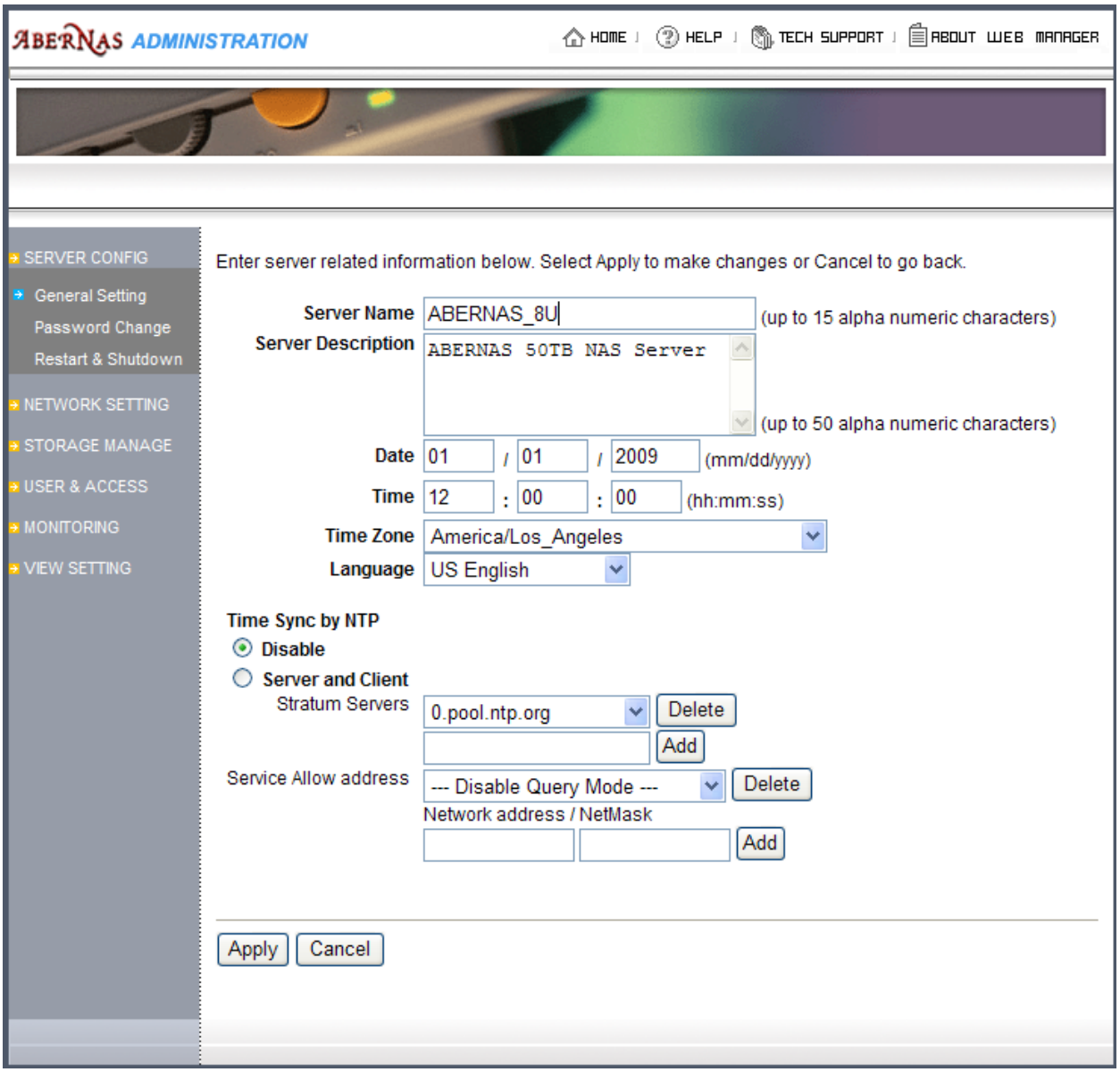
Manage – Edit Server Configuration, Network Settings, Storage Management, Add/Delete Users and Edit Access Settings, Monitor Server Activity Log, View Settings

Backup, Mirror and Restore – Edit Snapshot and Restore Settings, Edit Failover and Mirror Settings, Folder Replication, View Settings

Update – Apply Latest Patches and Updates, Log out of the Web Administration

Web Administration Interface > MANAGE > Server Config > General Settings –

Enter basic server information here such as server name, date, time and language. The AberNAS records the date and time of events, files and folders based on the system date & time set on this page.



Server Name - Enter a unique name to identify the ABERNAS server. Up to 15 alphanumeric characters (without spaces) are allowed for the server name.

Server Description - Enter a description of up to 50 alphanumeric characters for this ABERNAS to help identify its use. This is an optional field.

Date - Enter the system date in each appropriate field in the mm/dd/yyyy format. For example, you would enter 04192002 for April 19, 2002.

Time - Enter system time in the 4-hour format. Indicate hour, minutes and seconds in the hh:mm:ss format.

Time Zone - Select the time zone from the pull down menu. The default setting is US/Pacific Standard Time.

Language - The default language is US English. If you wish to support a different language, select the language from the pull down menu. This multiple language setting allows users to store and retrieve file and directory names that are in the selected language and US English. You must re-boot the server upon changing language.

Synchronize with Preconfigured NTP (Network Time Protocol) Server:

1. Select the SERVER AND CLIENT radio button
2. Select an NTP server from the STRATUM SERVERS pull down menu then click Apply.

Synchronize with a Custom NTP (Network Time Protocol) Server:

1. Select the SERVER AND CLIENT radio button.
2. Input the IP address of the NTP server and select Add . Then click Apply.

Delete An Existing NTP (Network Time Protocol) Server:

1. Select the NTP server from the Stratum Servers pull down menu.
2. Click DELETE.

Provide NTP Synchronization Service To Attached Clients:

1. Select the SERVER AND CLIENT radio button to provide this service to clients

NOTE:
AberNAS and client must be in the same subnet.

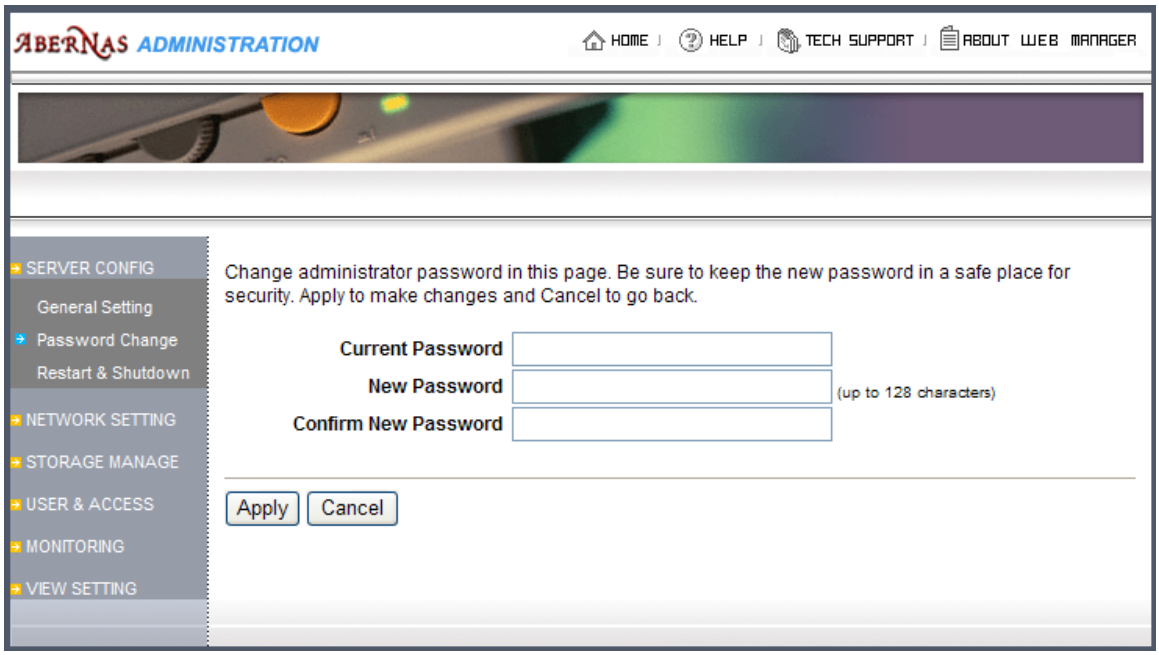
Provide NTP Synchronization Service To new Clients:

1. Select the SERVER AND CLIENT radio button.
2. Enter the IP Address and Netmask of the client in the Network Address/Netmask fields.
3. Click Add.

NOTE:
AberNAS and client must be in the same subnet.

After completing the general settings, Click APPLY to continue, or click CANCEL to discard changes and to return to the Administration Home Page.

Web Administration Interface > MANAGE > Server Config > Password Change –



To change your root login password, enter the following information into the fields shown above:

Current Password - Enter your current log-in password in this field.

NOTE:
For security, passwords you enter will be cloaked by asterisks (*) within all password fields.

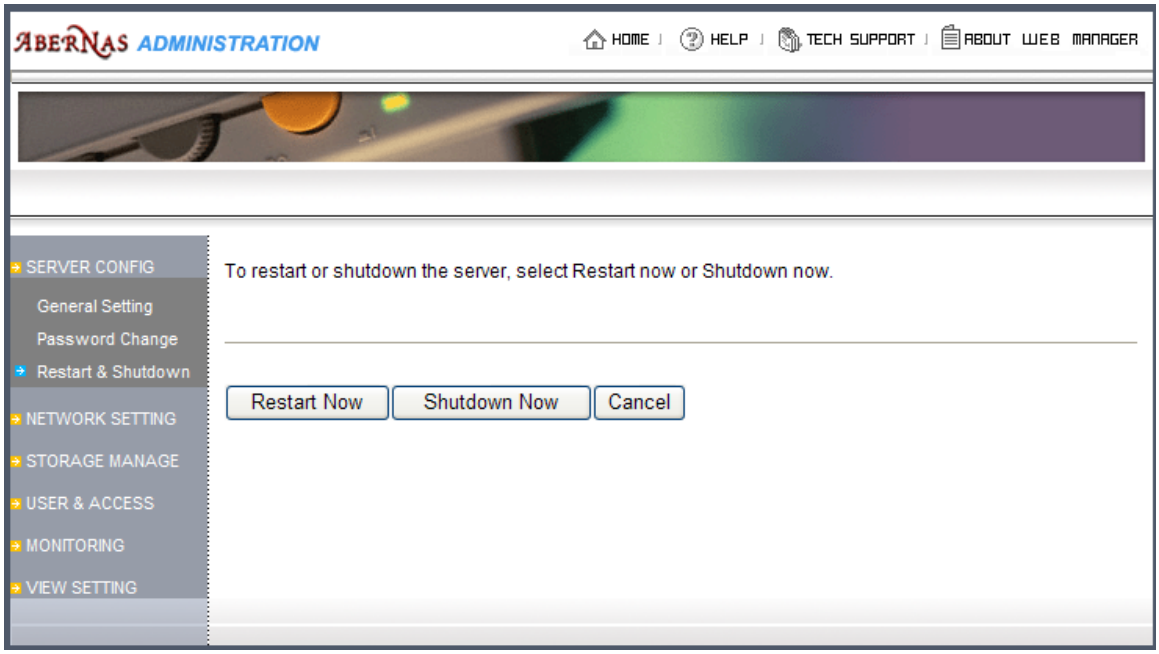
New Password - Enter a new password that consists of 6-8 alphanumeric characters. Non-alphanumeric characters such as \ @$ / –) # (* will not be accepted. Passwords are case-sensitive.

Confirm New Password - Re-enter the new password exactly as entered in the previous field.

CAUTION:
Be sure to record your password in a safe place. If you have forgotten your password, you are required to re-install the AberNAS OS. All data and configuration settings will be lost.

Click **APPLY** to complete the password change or Click **CANCEL** to discard the password change and return to the Administration Home Page.

Web Administration Interface > MANAGE > Server Config > Restart & Shutdown –



It may be necessary to restart the ABERNAS after system changes, upgrades, errors, etc.

NOTE:

All connected users are disconnected during restart & shutdown and can reconnect after the system reboots.

Restart now - Click this to shut down and reboot the ABERNAS system.

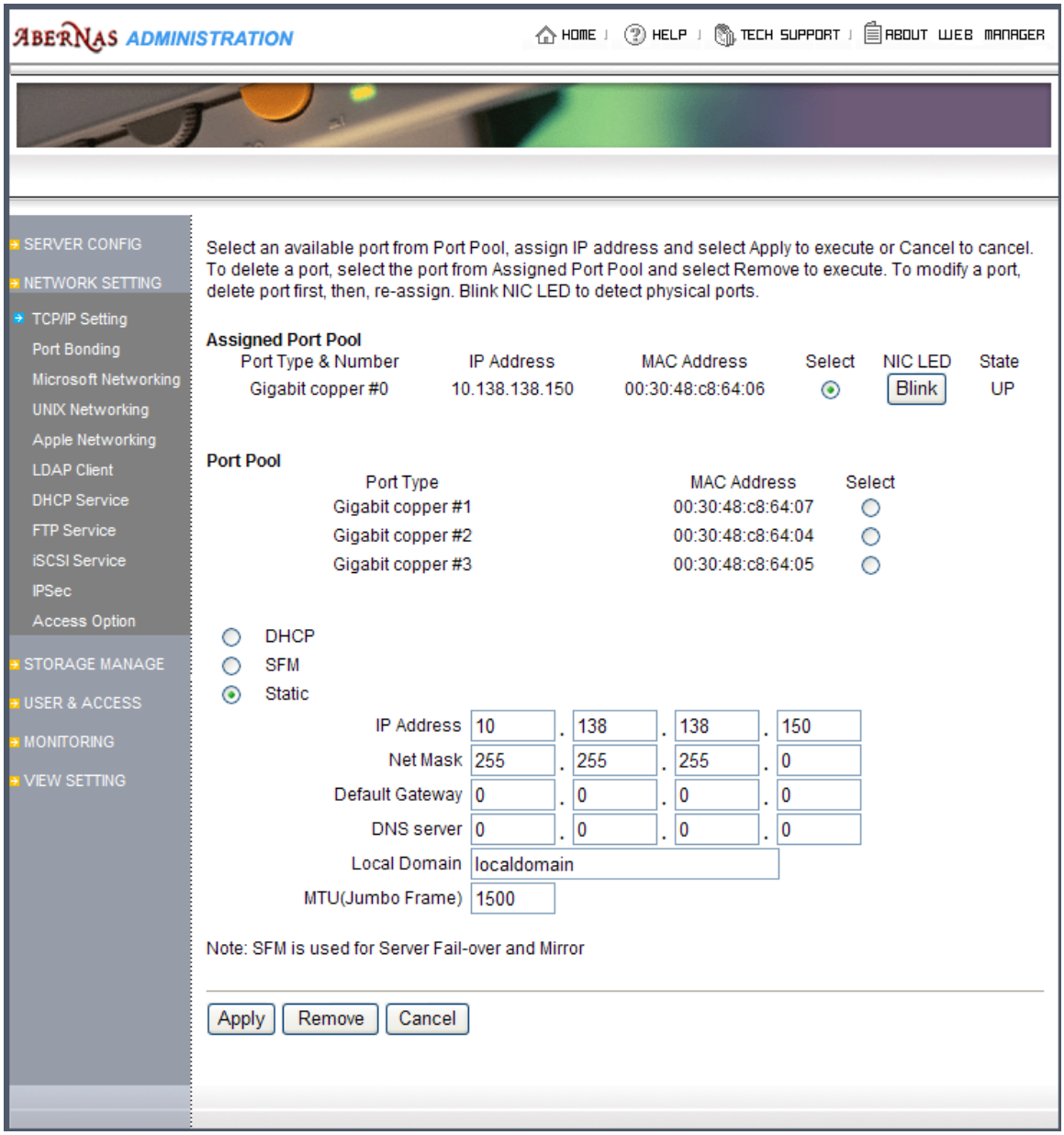
Shutdown Now - Click this to completely shut down the ABERNAS system. To manually force immediate shut down of the ABERNAS system, press the power button located on the front panel for more than four seconds.

NOTE:

After selecting the SHUTDOWN NOW button, the AberNAS system may undergo a short shut down process before turning off.

Cancel - Click this to return to the Administration Home without restarting or shutting down.

Web Administration Interface > MANAGE > Network Setting > TCP/IP Setting –



NOTE:

Multiple Gigabit ports may be configured in the ABERNAS system.

Configuring TCP/IP to Gigabit Port(s):

1. Select a desired Gigabit port from the PORT POOL.
2. If necessary, select **BLINK** to map the listed port with its respective PHYSICAL PORT.
3. Select **STATIC**, **SFM**, or **DHCP** port types.

Static Port - Port with a specific IP address provided by the network router or name server. If selected from the PORT POOL, input the TCP/IP information in the appropriate fields.

NOTE:

Static Port is recommended for servers that will be accessed frequently by remote clients. The DHCP setting may cause clients to become disconnected when the AberNAS system obtains a new IP address from the DHCP server. When using patch v.070620 or later, please input DNS information if the ADS server name is not identical to the domain name. Not having the DNS information may cause the AberNAS to not synchronize with the ADS domain.

SFM (Server Fail-over & Mirror) - Dedicated port(s) that is used to connect primary and secondary AberNAS units for data mirroring and fail-over. This port is not used to transfer data to attached clients.

NOTE:

To configure the SFM port, simply select the available port, select the SFM radio button and click APPLY. No TCP/IP information is needed for the SFM port configuration.

DHCP - Allows the AberNAS to receive an IP address from a DHCP server existing in the network. It is recommended that the DHCP setting is used for configuring the AberNAS system.

NOTE:

For DHCP, TCP/IP information input is not needed.

4. Click **APPLY** to complete this process. New Gigabit port settings will appear in the Assigned Port Pool. Click **CANCEL** to discard the changes and return to the Administration Home Page.

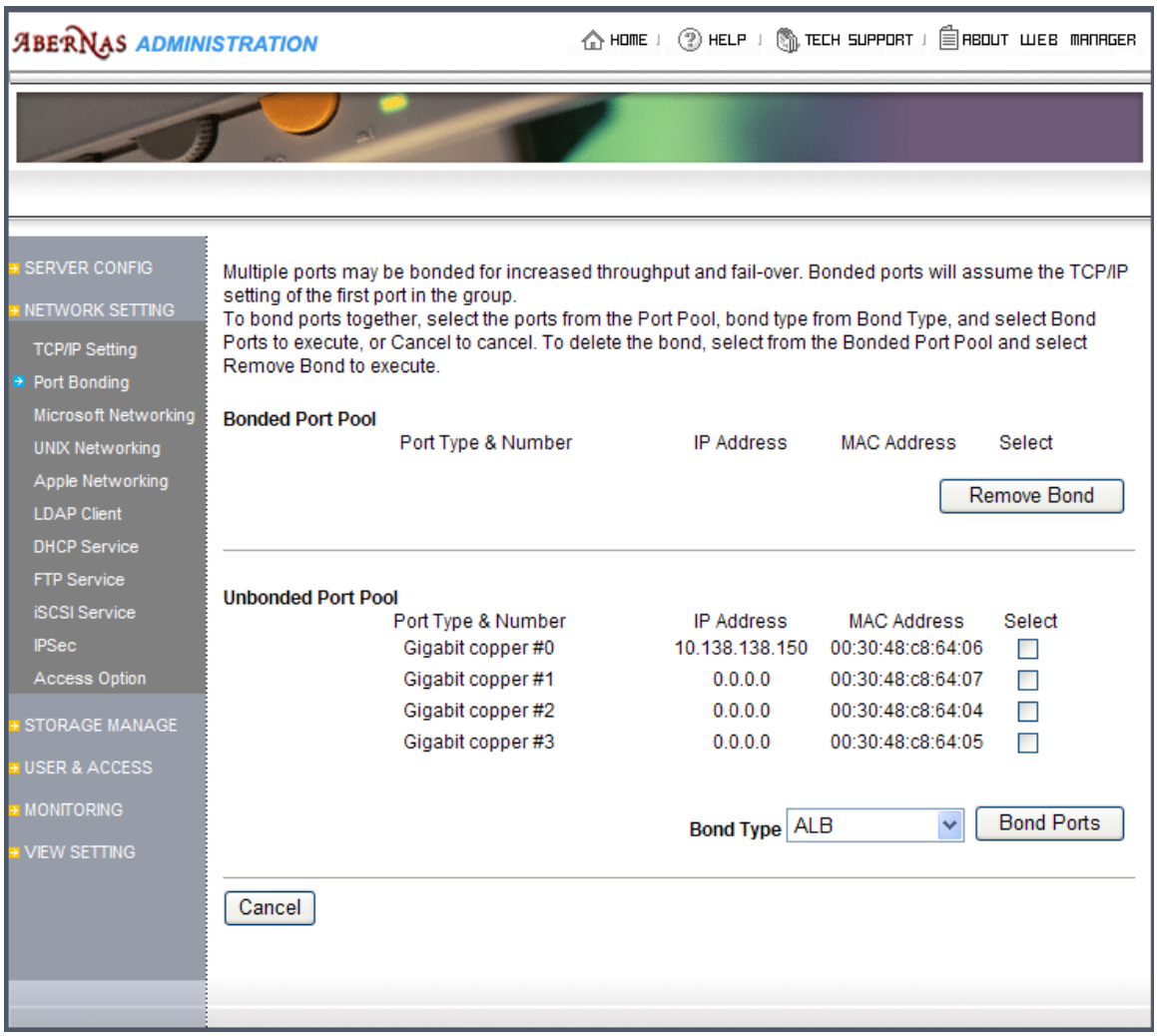
Remove a Port:

1. Select a desired Gigabit port from ASSIGNED PORT POOL. If necessary, select **BLINK** to map the listed port with the respective physical port.

2. Click **REMOVE** to remove the selected port or Click **CANCEL** to discard the changes and return to the Administration Home Page. The removed port will no longer be listed in the ASSIGNED PORT POOL.

Web Administration Interface > MANAGE > Network Setting > Port Bonding –

Multiple NIC ports may be bonded using one of seven different bonding methods. Bonded ports provide higher throughput as well as different levels of failover. All bonded ports assume the IP address and MAC address of the first port in the bond.



Bond Ports:

1. From the **UNBONDED PORT POOL**, select the desired ports you wish to bond.

2. Select the desired bonding method from the **BOND TYPE** pull down menu.

3. Click **BOND PORTS** to complete the configuration or Click **CANCEL** to discard the changes and return to the Administration Home Page. Any bonded ports will now show as a team under the BONDED PORTS POOL.

NOTE**:**

IP addresses for SFM ports are assigned internally. SFM can be viewed in the IP address section.

Remove Bond:

1. From the BONDED PORTS POOL, select the bonded team to remove.

2. Click **REMOVE BOND** to complete removal of port or click **CANCEL** to discard the changes and return to the Administration Home Page.

Bond Type Definitions:

Adaptive Load Balancing - Includes *balance-tlb* + receive load balancing (RLB) for IPV4 traffic and does not require any special switch support. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP replies sent by the server on their way out and overwrites the SRC HW address with the unique HW address of one of the slaves in the bond such that different clients use different HW addresses for the server.

Receive traffic from connections created by the server is also balanced. When the server sends an ARP Request the bonding driver copies and saves the client's IP information from the ARP. When the ARP Reply arrives from the client, its HW address is retrieved and the bonding driver initiates an ARP reply to this client assigning it to one of the slaves in the bond. A problematic outcome of using ARP negotiation for balancing is that each time that an ARP request is broadcasted it uses the HW address of the bond. Hence, clients learn the HW address of the bond and the balancing of receive traffic collapses to the current slave. This is handled by sending updates (ARP Replies) to all the clients with their assigned HW address such that the traffic is redistributed. Receive traffic is also redistributed when a new slave is added to the bond and when an inactive slave is re-activated. The receive load is distributed sequentially (round robin) among the group of highest speed slaves in the bond. When a link is reconnected or a new slave joins the bond the receive traffic is redistributed among all active slaves in the bond by initiating ARP Replies with the selected MAC Address to each of the clients. The up delay mode probe parameter must be set to a value equal or greater than the switch's forwarding delay so that the ARP replies sent to the clients will not be blocked by the switch.

802.3ad Dynamic Link Aggregation - Creates aggregation groups that share the same speed and duplex settings. Transmits and receives on all slaves in the active aggregator.

Pre-requisites:

1. Ethtool support in the base drivers for retrieving the speed and duplex of each slave.
2. A switch that supports IEEE 802.3ad dynamic link aggregation.

Round-Robin - Transmit in a sequential order from the first available slave through the last. This mode provides load balancing and fault tolerance.

Active-Backup - Only one slave in the bond is active. A different slave becomes active if, and only if, the active slave fails. The bond's MAC address is externally visible on only one port (network adapter) to avoid confusing the switch. This mode provides fault tolerance.

XOR - Transmit based on (source MAC address XOR'd with destination MAC address) module slave count. This selects the same slave for each destination MAC address. This mode provides load balancing and fault tolerance.

Broadcasting - Transmits everything on all slave interfaces. This mode provides fault tolerance.

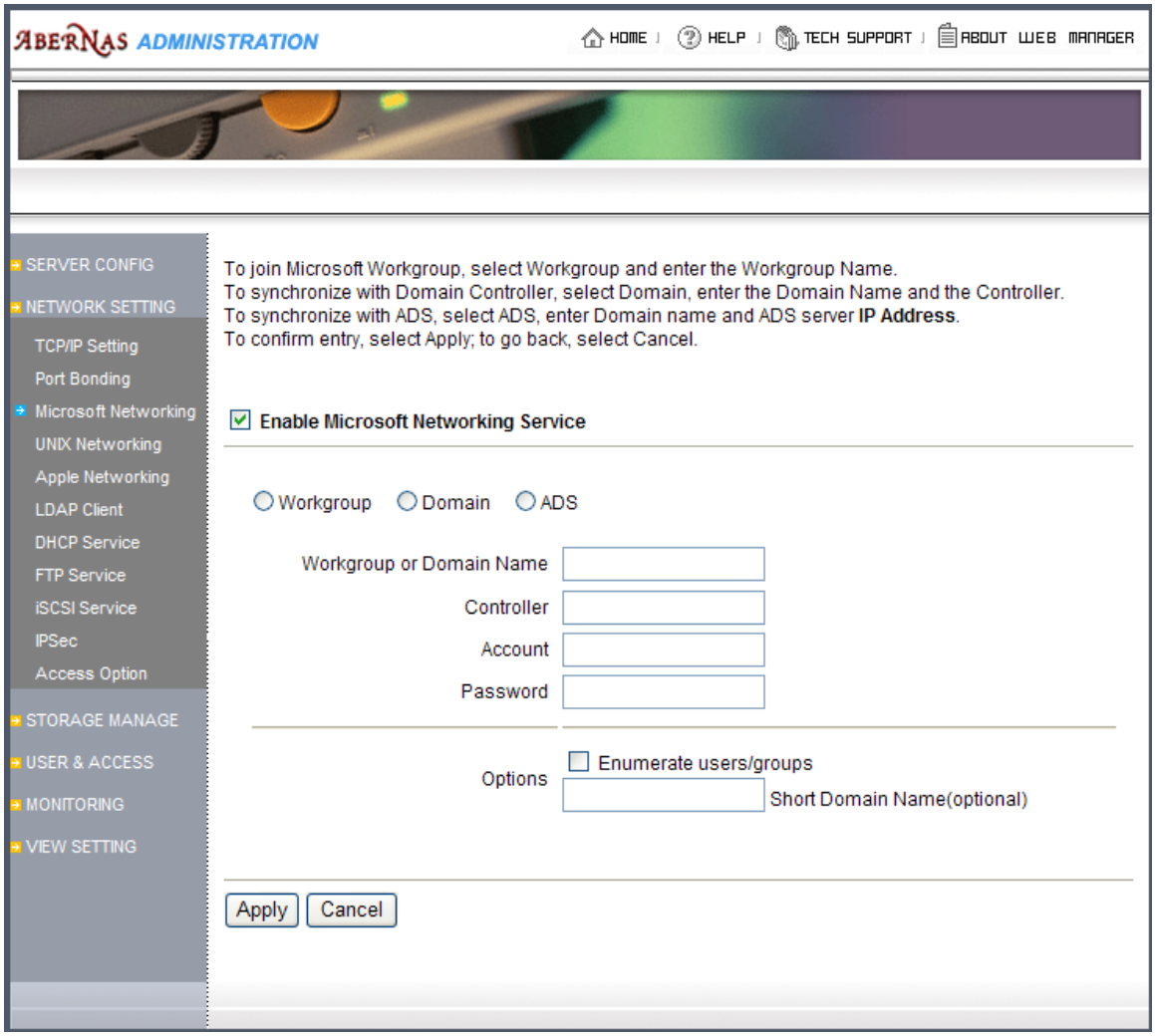
TLB (Transmit Load Balancing) - Channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the

speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC Address of the failed receiving slave.

Prerequisites:

1. Ethtool support in the base drivers for retrieving the speed of each slave.

Web Administration Interface > MANAGE > Network Setting > Microsoft Networking –



By default, Microsoft users and user groups (CIFS/SMB) are given access to AberNAS logical volumes. **Enable Microsoft Networking Service** is automatically selected by default.

Enable/disable CIFS/SMB Service:

1. Check or uncheck the **Enable Microsoft Networking Service** to enable or disable the service.

Join Microsoft Workgroup:

1. Select **WORKGROUP** networking radio button.
2. Enter the Workgroup name in the WORKGROUP OR DOMAIN NAME field.
3. Click **APPLY** to complete this process or click **CANCEL** to discard the changes and return to the Administration Home Page.

Join Microsoft Primary Domain Controller (PDC):

1. Select **DOMAIN** radio button.
2. Enter the domain name in the WORKGROUP OR DOMAIN NAME field.

3. Enter the name of the PDC in CONTROLLER field.

NOTE:

A Primary Domain Controller (PDC) must be available on your network.

4. Enter the Administrator account name and password in the ACCOUNT/PASSWORD fields.
5. Click **APPLY** to complete this process or Click CANCEL to discard the changes and return to the Administration Home Page. Upon successful synchronization with PDC, **"PDC sync. successful"** will appear.

NOTE:

Synchronizing with PDC or ADS will place all users and user groups in the PDC or ADS server in the AberNAS. When access to the AberNAS is attempted by either PDC or ADS users, the AberNAS will communicate with the PDC or ADS server to authenticate the user and pass through the proper permission. PDC and ADS synchronization cannot exist simultaneously. If synchronization to PDC or ADS fails, reset the AberNAS account from the PDC or ADS server and retry. In some cases, resetting the administrator's password resolves this problem. The AberNAS seeks and lists users and groups in local, LDAP, NLS, and ADS/PDC. In the event of duplicate user IDs, the users and groups will be listed in this order for selection: Local, LDAP, NIS, and ADS/PDC.

Join Microsoft Active Directory Service (ADS):

1. Select **ADS** radio button.
2. Enter the domain name in the WORKGROUP OR DOMAIN NAME field
3. Enter the IP address of the ADS server in the CONTROLLER field.

NOTE:

An active directory service (ADS) must be available in your network.

4. Enter the Administrator account name in the ACCOUNT field and password in the PASSWORD field.
5. Click **APPLY** to complete this process or click **CANCEL** to discard the changes and return to the Administration Home Page. Upon successful synchronization with ADS, **"ADS sync. successful"** will appear.

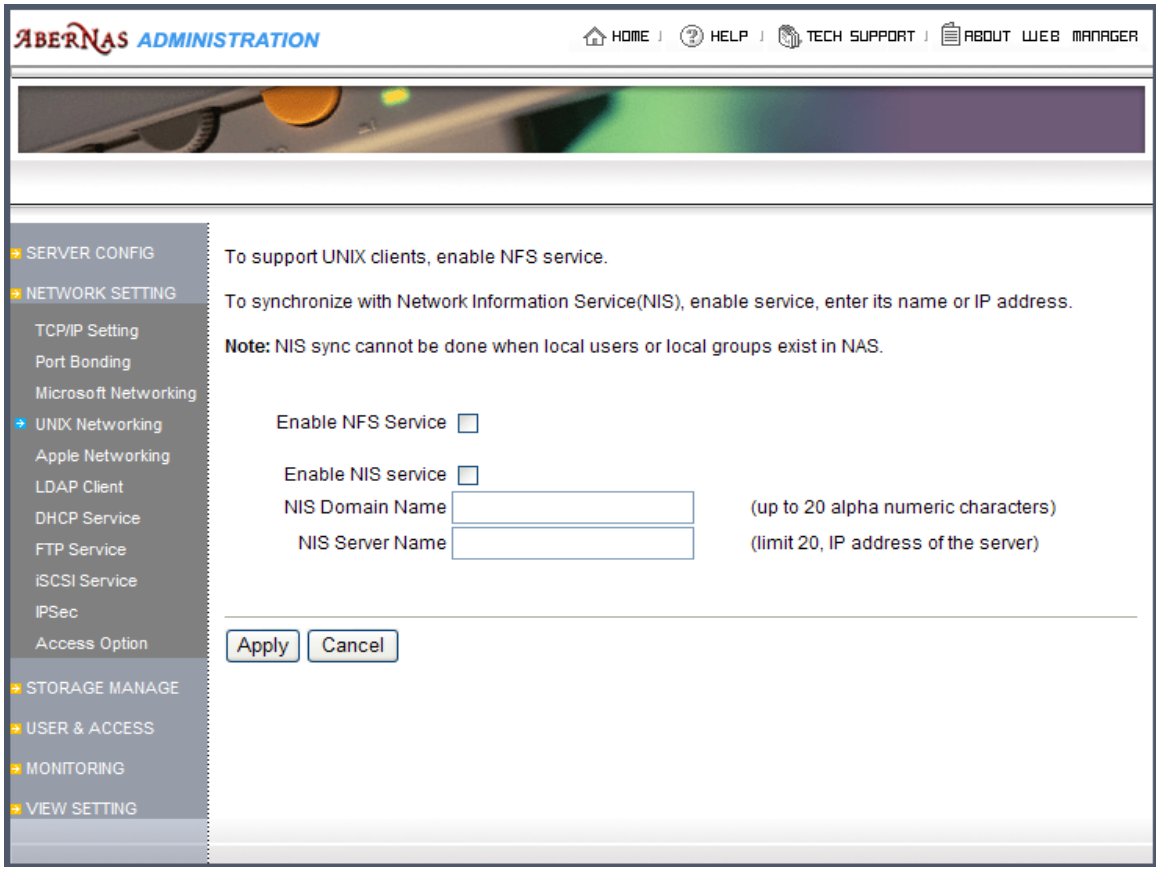
NOTE:

Synchronizing with PDC or ADS will place all users and user groups in the PDC, or ADS server in the AberNAS system (see all Users list in the Users & access: Microsoft page of the web administration interface). When access to the AberNAS is attempted by either PDC or ADS users, the AberNAS will communicate with the PDC or ADS server to authenticate the user and pass through the proper permission. PDC and ADS synchronization cannot exist simultaneously. In the case that synchronization to PDC or ADS fails, reset the AberNAS account from the PDC or ADS server and retry. Sometimes, resetting the administrator's password resolves the synchronization problem. The AberNAS may also fail to synchronize with ads if the system times for the AberNAS and ADS servers differ. Time for the AberNAS and the ADS server must be the same down to the minute. Check your input for domain name, server IP Address (or name for PDC), user ID and password. For AberNAS units updated with patch v.070620 or later, please input DNS information if the ADS server name is not identical to domain Name. Not having the DNS information may cause the AberNAS to not synchronize with ADS domain. The AberNAS seeks and lists users and groups in local, LDAP, NIS, and ADS/PDC. In the event where you have duplicate user IDs, the above order will be used to list and accept duplicate users and groups.

CAUTION:

When using SFM configuration, enable ADS synchronization before turning on SFM. If ADS synchronization should require disabling, disable SFM before disabling ADS synchronization.

Web Administration Interface > MANAGE > Network Setting > UNIX Networking –



In order to allow UNIX clients to access ABERNAS logical volumes, the NFS (Network File System) service must be enabled by checking the **ENABLE NFS SERVICE** check box. Synchronizing with NIS server will place all the users and user groups stored in the NIS server as local users and local user groups in the ABERNAS system. The ABERNAS will communicate with the NIS server to update the user and user group list. In addition, any access attempts made by the NIS users to the ABERNAS logical volume will be authenticated by the user ID and password stored in the NIS server.

Synchronize with Network Information Service (NIS):

1. Check **ENABLE NFS SERVICE** check box.
2. Check **ENABLE NIS SERVICE** check box.
3. Enter domain name in NIS DOMAIN NAME field.
4. Enter the NIS server name in the NIS SERVER NAME field.
5. Click **APPLY** to complete the process or click **CANCEL** to discard the changes and return to the Administration Home Page.

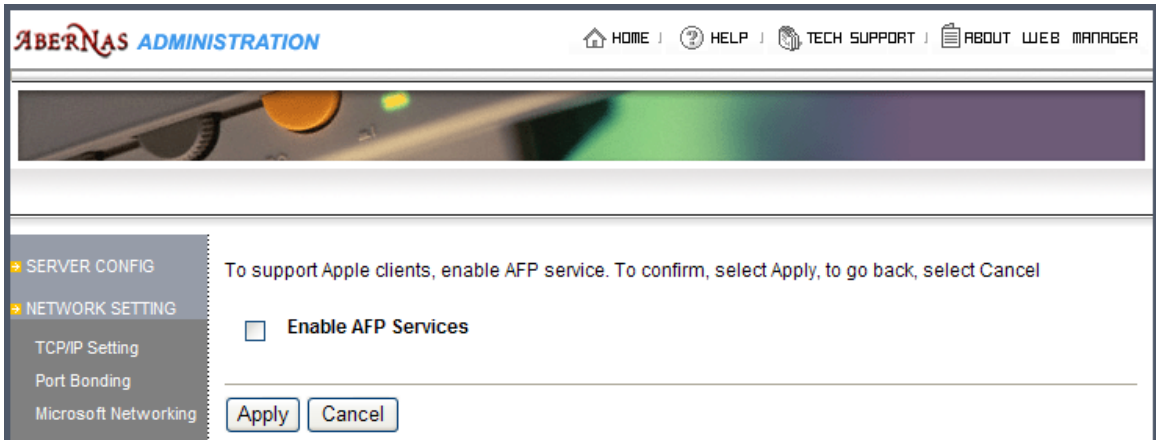
NOTE:

The AberNAS seeks and lists users and groups in local, LDAP, NIS, and ADS/PDC. In the event where you have duplicate user IDs, the above order will be used to list and accept duplicate users and groups.

CAUTION:

When using SFM configuration, enable NIS synchronization before turning on SFM. If NIS synchronization should require disabling, disable SFM before disabling NIS synchronization.

Web Administration Interface > MANAGE > Network Setting > Apple Networking –



Allow Apple Clients To Access AberNAS Logical Volumes:

1. Turn on the AFP service by enabling **AFP SERVICE** check box.

NOTE:

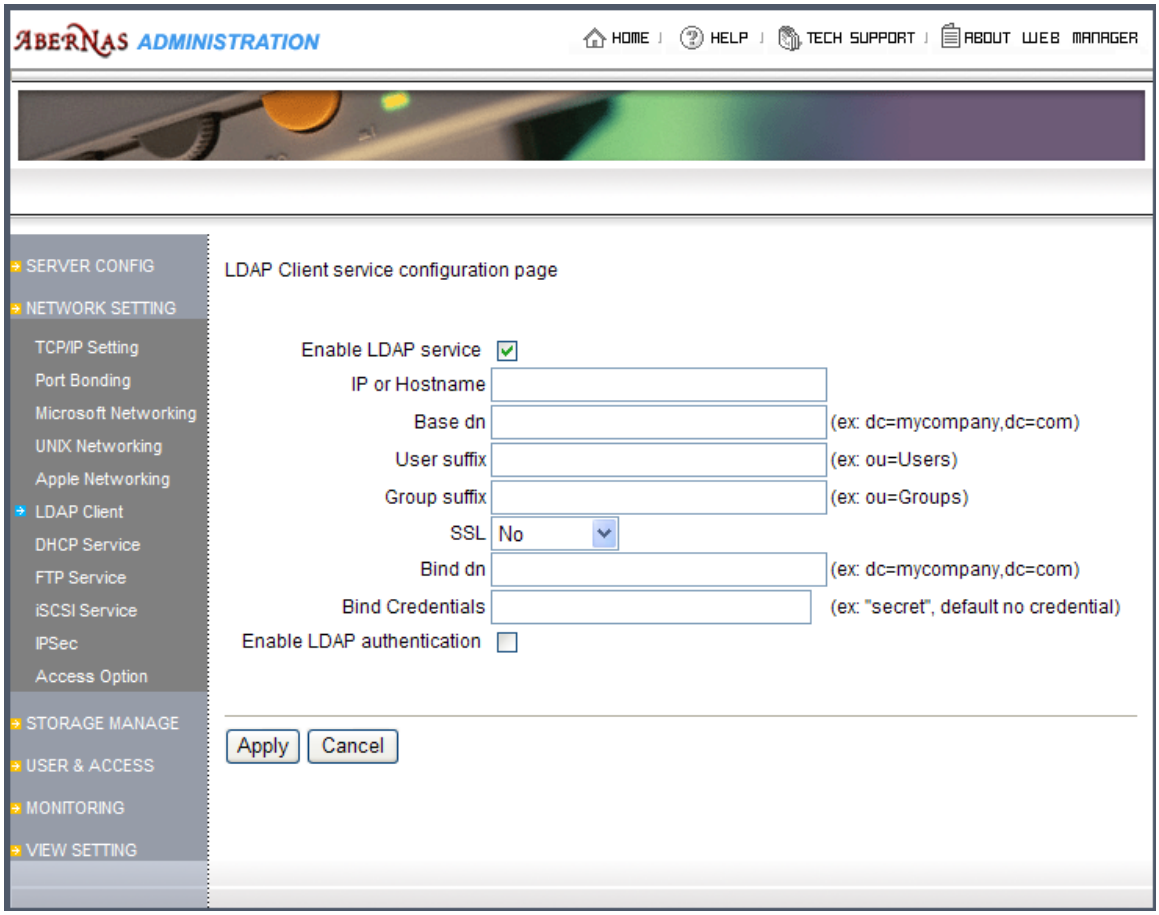
The AFP service will allow local users and user groups of AberNAS or NIS users and user groups to access AberNAS logical volumes.

2. Click **APPLY** to complete the process or click **CANCEL** to discard the changes and return to the Administration Home Page. If Apple clients cannot be mounted, especially OS versions 9.x, to the ABERNAS, enter the following command:

rm /usr/local/etc/netatalk/afpd.conf init 6

The system will reboot and attempt to mount to the network share again.

Web Administration Interface > MANAGE > Network Setting > LDAP Client –



LDAP (Lightweight Directory Access Protocol) is a protocol used to access network directory. The ABERNAS supports LDAP.

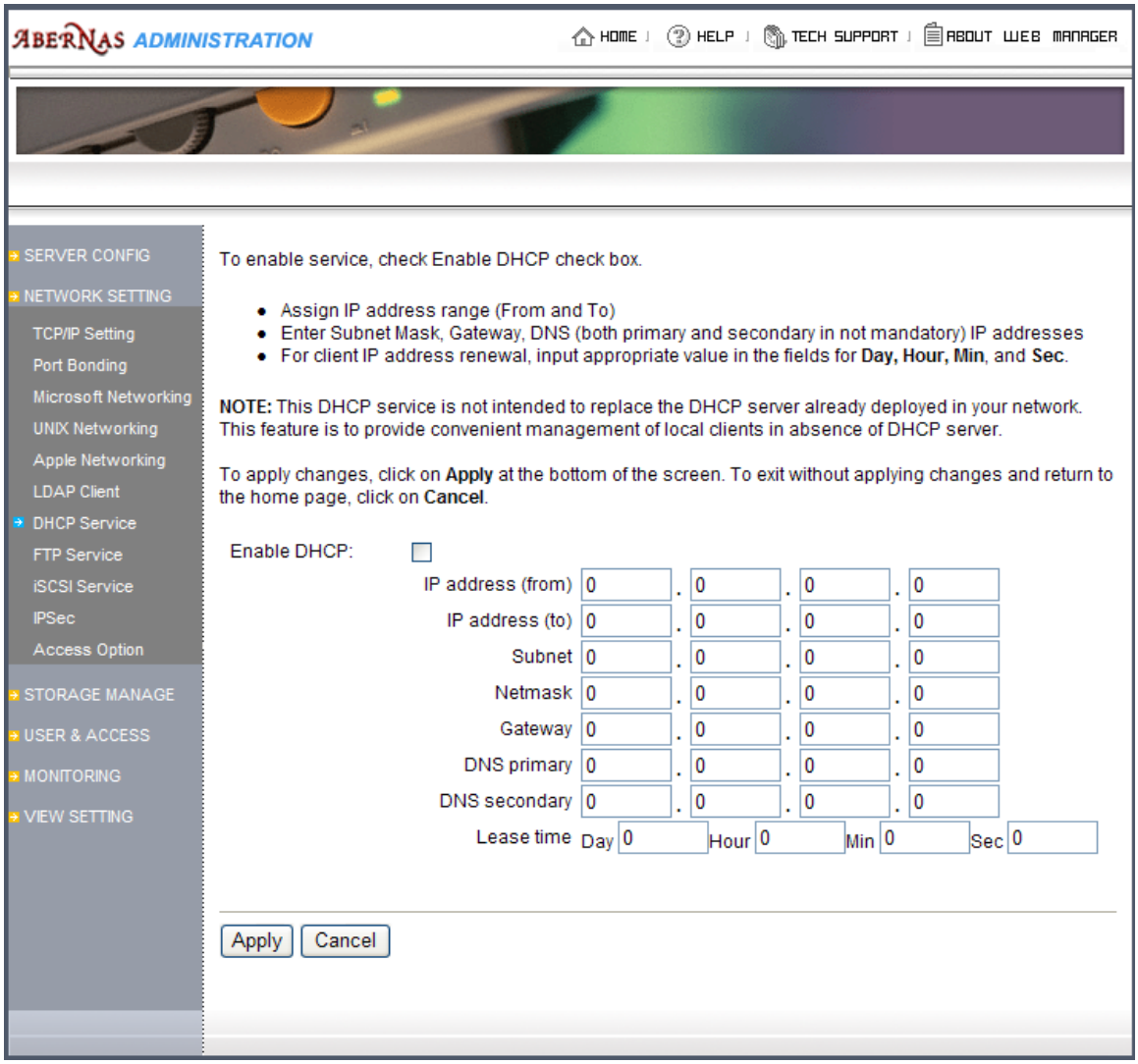
Configure LDAP Client Service:

1. Enable the **ENABLE LDAP SERVICE** check box to access the LDAP server.
2. Enter IP or host name of the LDAP server in IP or HOST NAME field.
3. Input company and extension in BASE DN field.
(Example: dc=mycompany, dc=com)
4. Input ID and extension to access the LDAP server in BIND DN field.
(Example: dc=administrator,dc=AberNAS1)
5. Input password required to access the LDAP server in BIND CREDENTIALS field.
(Example: ***secret***. The default setting is a blank field.
6. Click **APPLY** to complete or click **CANCEL** to discard the changes and return to the Administration Home Page. Upon synchronization, user list will be listed in the Local User and Local User Group list.

NOTE:

The AberNAS seeks and lists users/groups in local, LDAP, NIS, and ADS/PDC. In the event where you have duplicate user IDs, the above order will be used to list and accept duplicate users and groups.

Web Administration Interface > MANAGE > Network Setting > DHCP Service –



The DHCP service on the AberNAS can be used to assign IP addresses to the attached clients.

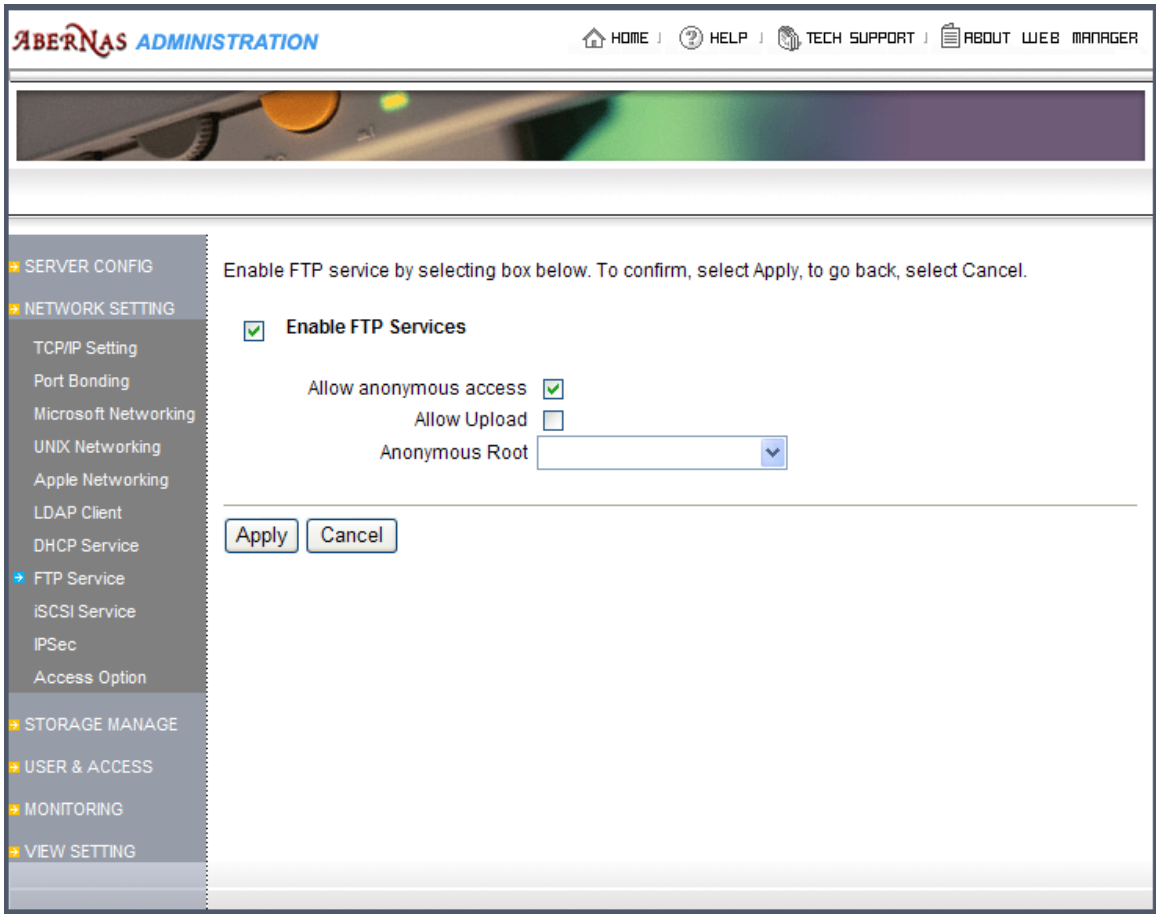
Enable DHCP Service:

1. Check **ENABLE DHCP** check box.
2. Assign IP Address range.
3. Enter Subnet.
4. Enter Gateway.
5. Enter addresses for DNS primary and/or DNS secondary. Entering both primary and secondary is not absolutely required.
6. For client IP address renewal, input appropriate value in the fields for Day, Hour, Min, and Sec.
7. Click **APPLY** to complete this process or click **CANCEL** to discard the changes and return to the Administration Home Page.

NOTE:

The DHCP service on the AberNAS is not intended to replace the DHCP server of the Active Directory Service, Primary Domain Controller or Network Information Service. This feature is to provide convenient management of local clients that are not part of aforementioned network infrastructure.

Web Administration Interface > MANAGE > Network Setting > FTP Service –



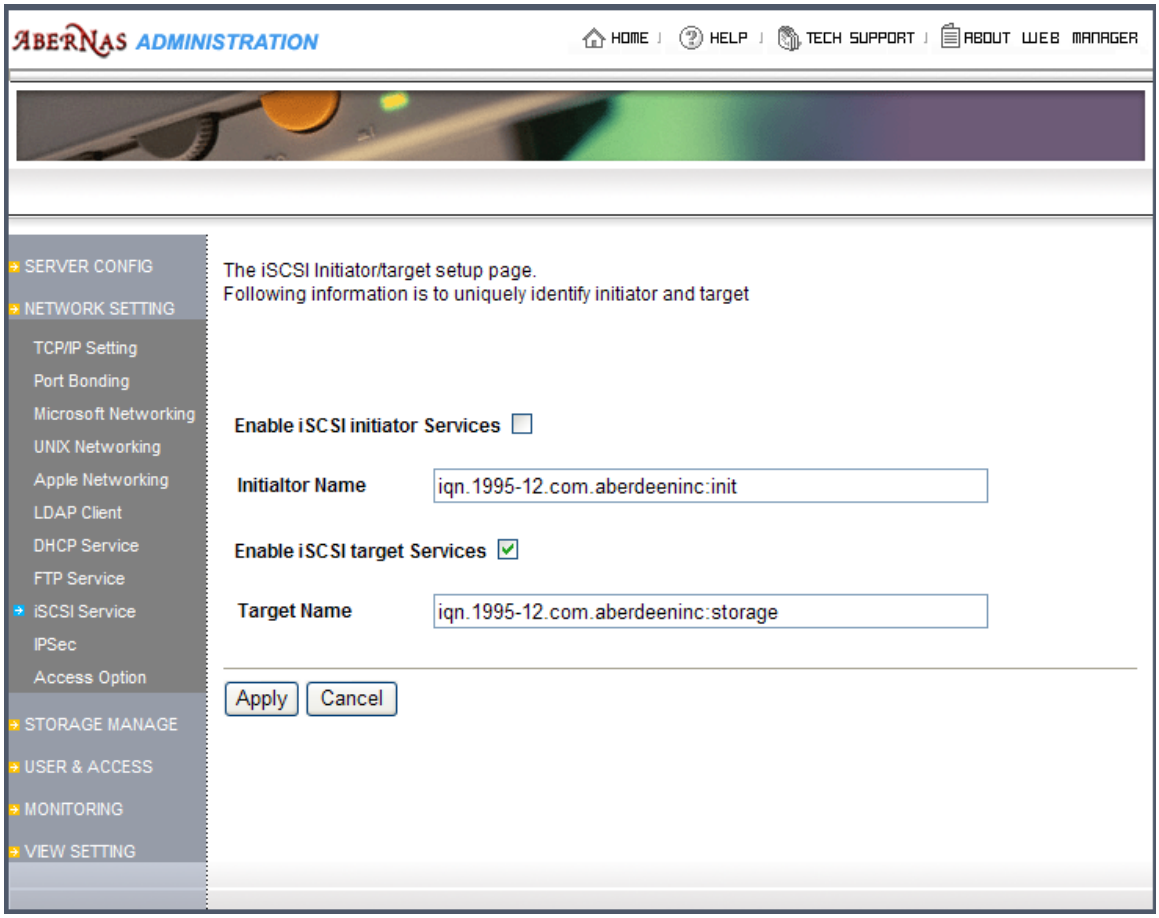
Enable FTP Service:

1. Select **ENABLE FTP SERVICE** check box to allow FTP access to remote users.
2. Select **ALLOW ANONYMOUS ACCESS** to allow any user to access public directories via FTP.
3. Enable **ALLOW UPLOAD** to give privileged ability to read/write to public directories via FTP.
4. Select the Logical Volume where the public FTP directory will reside from the ANONYMOUS ROOT pull down menu.
5. Click **APPLY** to complete or click **CANCEL** to discard the changes and return to the Administration Home Page.

NOTE:

For security, it is recommended that the FTP service is provided behind a properly configured firewall to avoid unwanted intrusion over the network.

Web Administration Interface > MANAGE > Network Setting > iSCSI Service –



The ABERNAS is equipped with iSCSI initiator and target services that attach multiple iSCSI target devices and converts them to Logical Volumes for client access. iSCSI target devices can reside within the ABERNAS, or in external systems.

Enable the iSCSI Initiator Service:

1. Select the **ENABLE iSCSI INITIATOR SERVICE** check box to start the initiator service.
2. To change the default initiator name, enter the new name in the INITIATOR NAME field.

NOTE:

iSCSI names must be built in accordance with specific iSCSI node naming rules in order to function properly. Here is a summary of the rules:

A. Node names are encoded in the UTF-8 character set. Note the initiator service does not support UCS-4 characters. RFC 2044 describes UTF-8 encoding.
B. Node names are 223 bytes or less.
C. Node names may contain alphabetic characters (a to z), numbers (0 to 9) and three special characters: '.', '-', and ':'.
D. Uppercase characters are always mapped to lowercase.

Complete rules for building iSCSI node names are described in the iSCSI specification and the "String profile for iSCSI Names" internet draft.

3. Complete the instructions for enabling the iSCSI TARGET Service by completing the instructions below or Click **APPLY** to save the current settings. Click **CANCEL** to discard the changes and return to the Administration Home Page.

Enable the iSCSI Target Service:

1. Select the **ENABLE iSCSI TARGET SERVICE** check box.
2. Use the default name given in the TARGET NAME field or follow the requirements described in the iSCSI specification.
3. Click **APPLY** to complete or click **CANCEL** to discard the changes and return to the Administration Home Page.

Web Administration Interface > MANAGE > Storage Management – Overview

The ABERNAS system with an installed RAID controller can manage a broad range of storage devices for enhanced speed, added storage capacity to virtual disks and decreased impact of disk failure. Through the ABERNAS Web Administrator interface, the administrator can configure the installed RAID controller(s) to manage and format the internal and external storage devices.

The Storage Management interfaces in the Web Administrator allow the administrator to:

- Define the RAID type and format storage devices
- Use the iSCSI initiator to connect to external iSCSI devices
- Convert multiple individual fixed-disks into single large virtual storage volumes
- Increase the total storage capacity of virtual storage volumes

This section contains definitions for the terms and configurable settings found in the Storage Management interfaces of the Web Administration.

Definitions for Volume Group Types:

The ABERNAS system uses a hierarchical structure of storage volumes and volume groups in order to manage storage. The Web Administrator RAID Volume Manager provides the interface from which available storage devices can be implemented into this hierarchical structure of storage volumes:

Raw Volume (RV) – Raw Volumes are the unformatted fixed disks, SCSI and iSCSI target devices. In order to be used, RVs must be belong to a named volume group called Physical Volume (PV). Raw Volumes can only belong to a single Physical Volume. Before being assigned to a Physical Volume, any available Raw Volumes are grouped into an RV POOL.

Physical Volume (PV) – Physical Volumes are collections of 1 to 3 Raw Volumes of varying sizes and types that have been converted into a single virtual storage volume with the total storage capacity equaling the sum of its parts. Up to (**55)** Physical Volumes can be contained per system. All or a portion of the Physical Volumes can now be partitioned and formatted into Logical Volumes of varying sizes and types.

Logical Volume (LV) – Logical Volumes are the formatted partitions of the Physical Volumes that can be access by clients.

Definition of RAID Volume Types:

RAID 0 - Combining multiple disk drives, into a single RAID volume as if it were a single disk drive. Data is written across multiple disk drives which increases the performance of the disk I/O. RAID 0 requires minimum of disk drives and there's **no fault tolerance** built into the RAID. Any single disk drive failure will cause the entire RAID to fail. Capacity of RAID 0 is equal to the available capacity of all the disk drives combined within the RAID.

RAID 1 - Pairing of disk drives such that data is written to both drives. This creates redundancy in data so that failure of either disk drive will not cause total loss of data or access to the data. There's no disk I/O performance gain for RAID 1. RAID 1 requires a minimum of two disk drives and the capacity of RAID 1 is equal to half of the available capacity of all the disk drives combined within the RAID.

RAID 3 - RAID 3 provides disk striping and complete data redundancy though a dedicated parity drive. RAID 3 breaks up data into smaller blocks, calculates parity by performing an exclusive-or

on the blocks, and then writes the blocks to all but one drive in the array. The parity data created during the exclusive-or is then written to the last drive in the array. If a single drive fails, data is still available by computing the exclusive-or of the contents corresponding strips of the surviving member disk. RAID 3 is best for applications that require very fast data- transfer rates or long data blocks.

RAID 5 - Combining three or more disk drives with striping and built-in parity that rotates amongst the configured drives. This allows data sustaining and recovery even after a single drive failure. Disk I/O performance is slower than other RAID levels due to heavier processing requirements. Capacity of RAID 5 is equal to the sum of all drives combined within the RAID minus one drive's available capacity.

RAID 6 - Provides the highest reliability. It is similar to RAID 5, but it performs two different parity computations or the same computation on overlapping subsets of the data. RAID 6 can offer fault tolerance greater than RAID 1 or RAID 5 but only consumes the capacity of 2 disk drives for distributed parity data. RAID 6 is an extension of RAID 5 but uses a second, independent distributed parity scheme. Data is striped on a block level across a set of drives, and then a second set of parity is calculated and written across all of the drives.

RAID 10 - Using four or more disk drives to pair drives, then stripe across the pairs. In essence, it is the combining of RAID 0 and RAID 1. This provides redundancy in data (due to the paring of drives and each having the same data) as well as an increase in disk I/O performance (due to striping across paired drives). Capacity of RAID 10 is ½ of available capacity of all drives combined within the RAID.

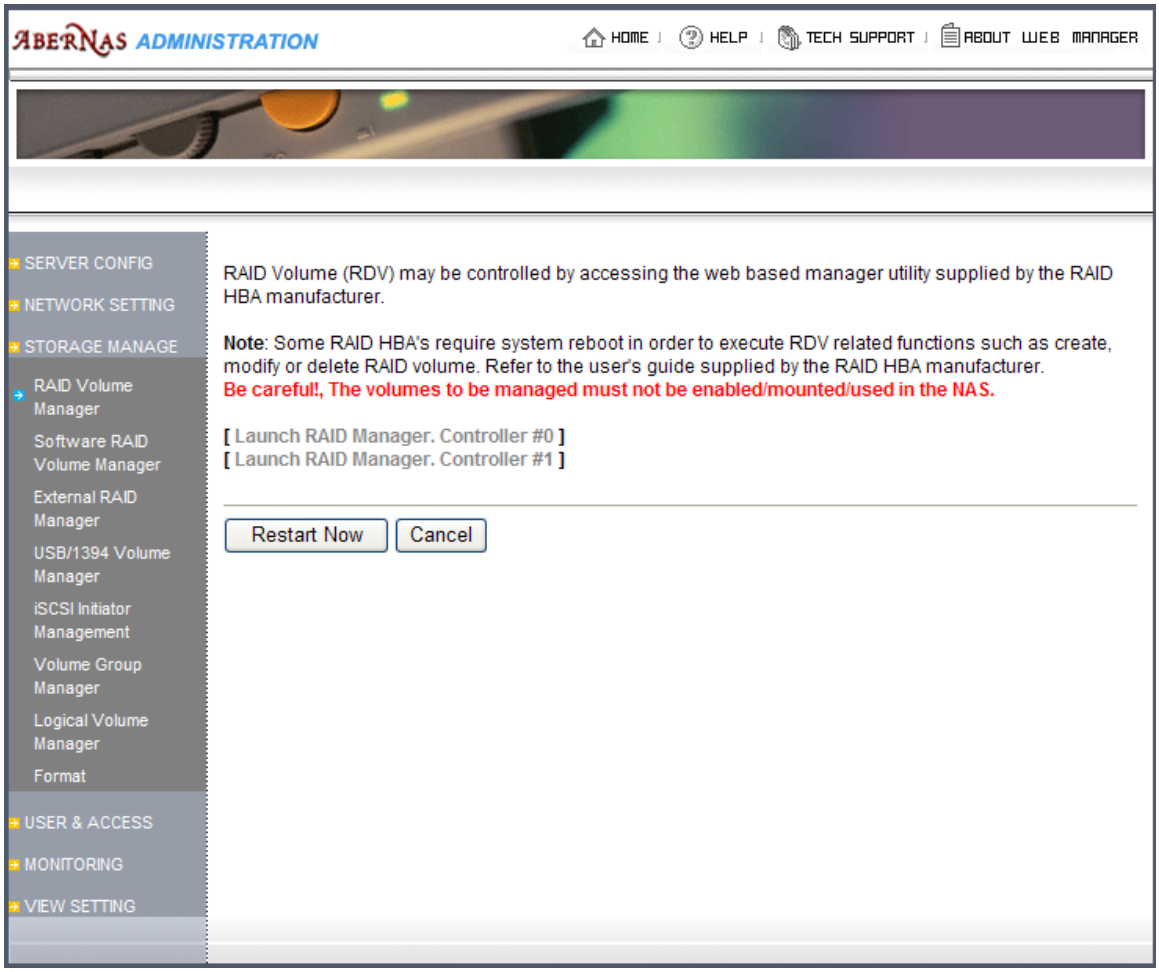
RAID x0 - RAID level x0 refers to RAID level 30, 50 and 60. RAID x0 is a combination multiple RAID x volume sets with RAID 0 (striping). Striping helps to increase capacity and performance without adding disks to each RAID x array. The operating system uses the spanned volume in the same way as a regular volume. Up to one drive in each sub-volume (RAID 3 or 5) may fail without loss of data. Up to two drives in each sub-volume (RAID 6) may fail without loss of data. RAID level x0 allows more physical drives in an array. The benefits of doing so are larger volume sets, increased performance and increased reliability.

Degraded - Means that the RAID volume is degraded. For example, if 1 of the drives in RAID 1 has failed, then this RAID 1 volume is known to be in a degraded state.

Rebuild - Means that a degraded RAID volume is being repaired to the normal state. Rebuild usually takes place when a hot spare or replacement disk, in place of the failed disk, is added to the degraded RAID volume.

Hot Spare – An active stand-by disk drive that is ready to replace any failed disk drive that belongs to a RAID volume. Hot spares prevent total loss of RAID volume in case of a single disk drive failure, allowing more time for the user to replace the failed disk drive.

Web Administration Interface > MANAGE > Storage Management – RAID Volume Manager


ABERNAS ADMINISTRATION
HOME
HELP
TECH SUPPORT
ABOUT WEB MANAGER
SERVER CONFIG
NETWORK SETTING
STORAGE MANAGE
RAID Volume Manager
Software RAID Volume Manager
External RAID Manager
USB/1394 Volume Manager
iSCSI Initiator Management
Volume Group Manager
Logical Volume Manager
Format
USER & ACCESS
MONITORING
VIEW SETTING
RAID Volume (RDV) may be controlled by accessing the web based manager utility supplied by the RAID HBA manufacturer.
Note: Some RAID HBA's require system reboot in order to execute RDV related functions such as create, modify or delete RAID volume. Refer to the user's guide supplied by the RAID HBA manufacturer.
Be careful!, The volumes to be managed must not be enabled/mounted/used in the NAS.
[Launch RAID Manager. Controller #0]
[Launch RAID Manager. Controller #1]
Restart Now
Cancel

Managing RAID Volumes:

The RAID Volume Manager page serves as a portal to the RAID controller's dedicated web administration GUI (Graphical User Interface). The number of RAID controllers shown on the page will vary based on the size of the AberNAS server. For example, a 1U AberNAS will have a single RAID Manager whereas an 8U AberNAS will have two.

Click on **Launch RAID Manager Controller #0 or #1** to manage the physical disks connected to each controller in the AberNAS. Changes made to the RAID configuration may require a reboot. Once changes are complete be sure to click **Restart Now** so any changes can be applied.

A separate user name and password will be required to login to the RAID Mangers and they are not the same as those used for the AberNAS system itself. The default user name and password for the AberNAS RAID Managers are shown below:

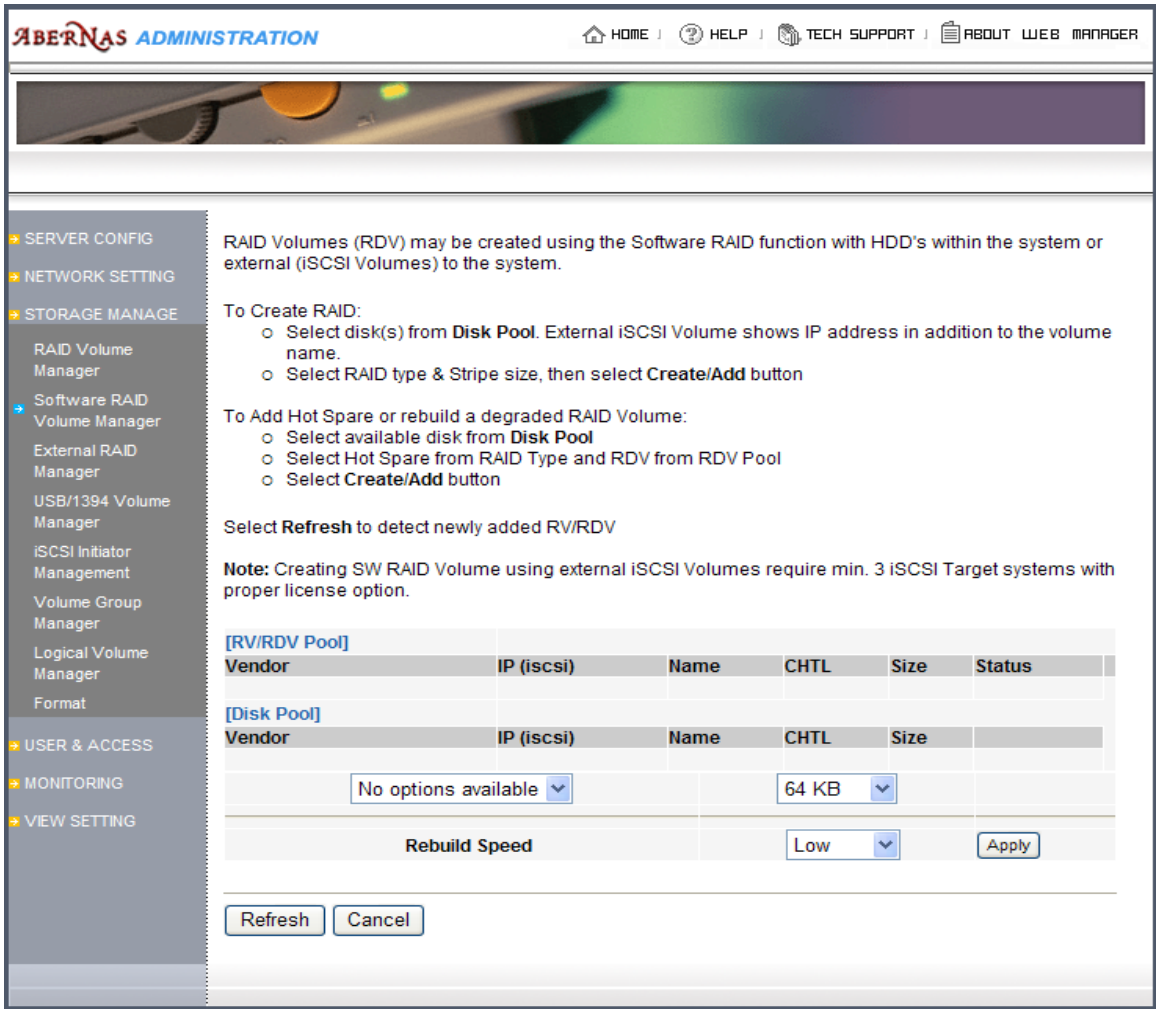
User Name: admin

Password: 0000

NOTE:

Please see appendix for complete RAID controller management guide.

Web Administration Interface > MANAGE > Storage Management – Software RAID Manager



Certain models of the AberNAS (2U and smaller) may have this page available in the **Storage Manage** section of the GUI. The Software RAID Manager is only used when no HW RAID controllers are used in the system or when external iSCSI volumes are connected.

RAID Volumes (RDV) may be created using the Software RAID function with HDD's within the system or external (iSCSI Volumes) to the system.

To Create RAID:

1. Select disk(s) from **Disk Pool.** (External iSCSI volume shows IP address in addition to the volume name)
2. Select RAID type & size. Select **Create/Add** button.

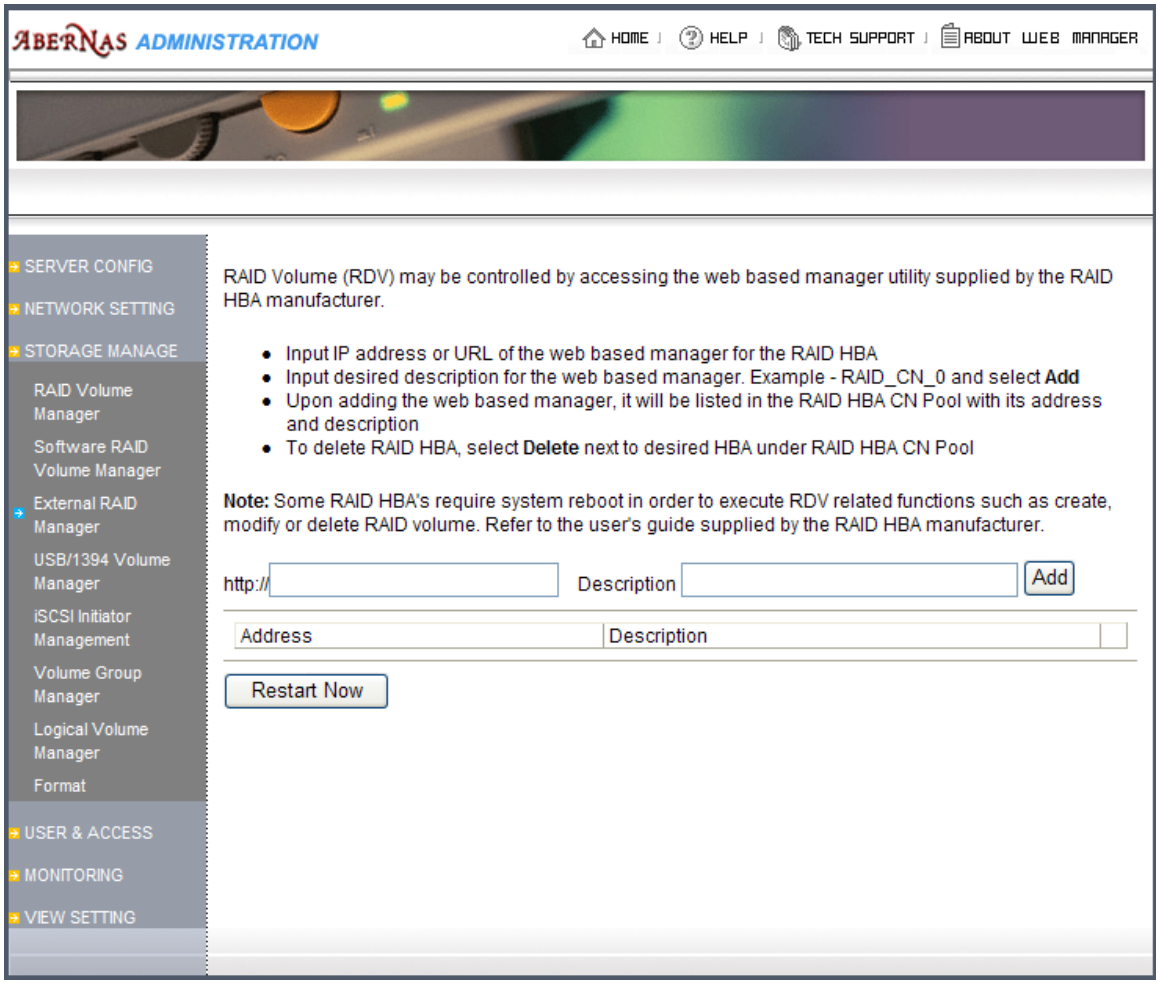
To Add Hot Spare or to rebuild a degraded RAID Volume:

1. Select available disk from **Disk Pool**
2. Select Hot Spare from RAID Type and RDV from RDV Pool
3. Select **Create/Add** button
4. Select Refresh to detect newly added RV/RDV

Note:

Creating SW RAID Volume using external iSCSI Volumes require min. 3 iSCSI Target systems with proper license option.

Web Administration Interface > MANAGE > Storage Management – External RAID Manager


ABERNAS ADMINISTRATION
HOME
HELP
TECH SUPPORT
ABOUT WEB MANAGER
SERVER CONFIG
NETWORK SETTING
STORAGE MANAGE
RAID Volume Manager
Software RAID Volume Manager
External RAID Manager
USB/1394 Volume Manager
iSCSI Initiator Management
Volume Group Manager
Logical Volume Manager
Format
USER & ACCESS
MONITORING
VIEW SETTING
RAID Volume (RDV) may be controlled by accessing the web based manager utility supplied by the RAID HBA manufacturer.
Input IP address or URL of the web based manager for the RAID HBA
Input desired description for the web based manager. Example - RAID_CN_0 and select Add
Upon adding the web based manager, it will be listed in the RAID HBA CN Pool with its address and description
To delete RAID HBA, select Delete next to desired HBA under RAID HBA CN Pool
Note: Some RAID HBA's require system reboot in order to execute RDV related functions such as create, modify or delete RAID volume. Refer to the user's guide supplied by the RAID HBA manufacturer.
http://
Description
Add
Address
Description
Restart Now

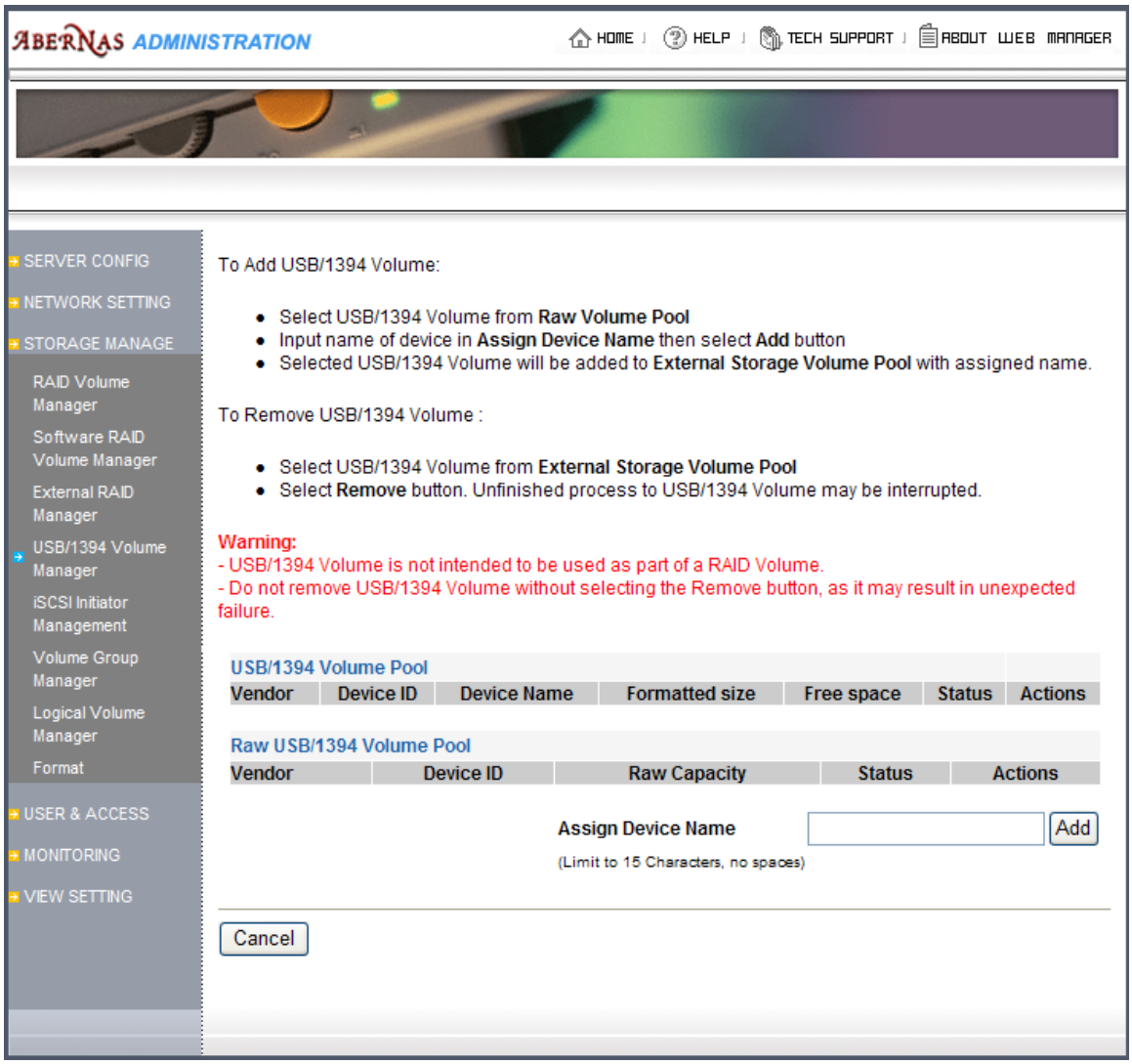
Certain models of the AberNAS (2U and Higher) may have this page available in the **Storage Manage** section of the GUI. The External RAID Manager serves as a shortcut to manage any Aberdeen XDAS units that may be connected to the AberNAS which would normally be managed by opening a separate web browser window. This enables the user to manage all RAID devices through a single management interface.

1. Input IP address or URL of the web based manager for the RAID HBA.
2. Input desired description for the web based manager. (Example: Aberdeen XDAS) Select **Add.**
3. Upon adding the web based manager, it will be listed in the RAID HBA CN Pool with its address and description.

Note:

Some RAID HBAs require system reboot in order to execute RDV related functions such as create, modify or delete RAID volume. Refer to the user's guide supplied by the RAID HBA manufacturer.

Web Administration Interface > MANAGE > Storage Management – USB/1394 Volume Manager



The USB/1394 Volume Manager is used to add external storage to the AberNAS so it can be shared out as network storage.

To Add USB/1394 Volume:

1. Select USB/1394 Volume from **Raw Volume Pool**
2. Input name of device in **Assign Device Name** then select **Add** button
3. Selected USB/1394 Volume will be added to **External Storage Volume Pool** with assigned name.

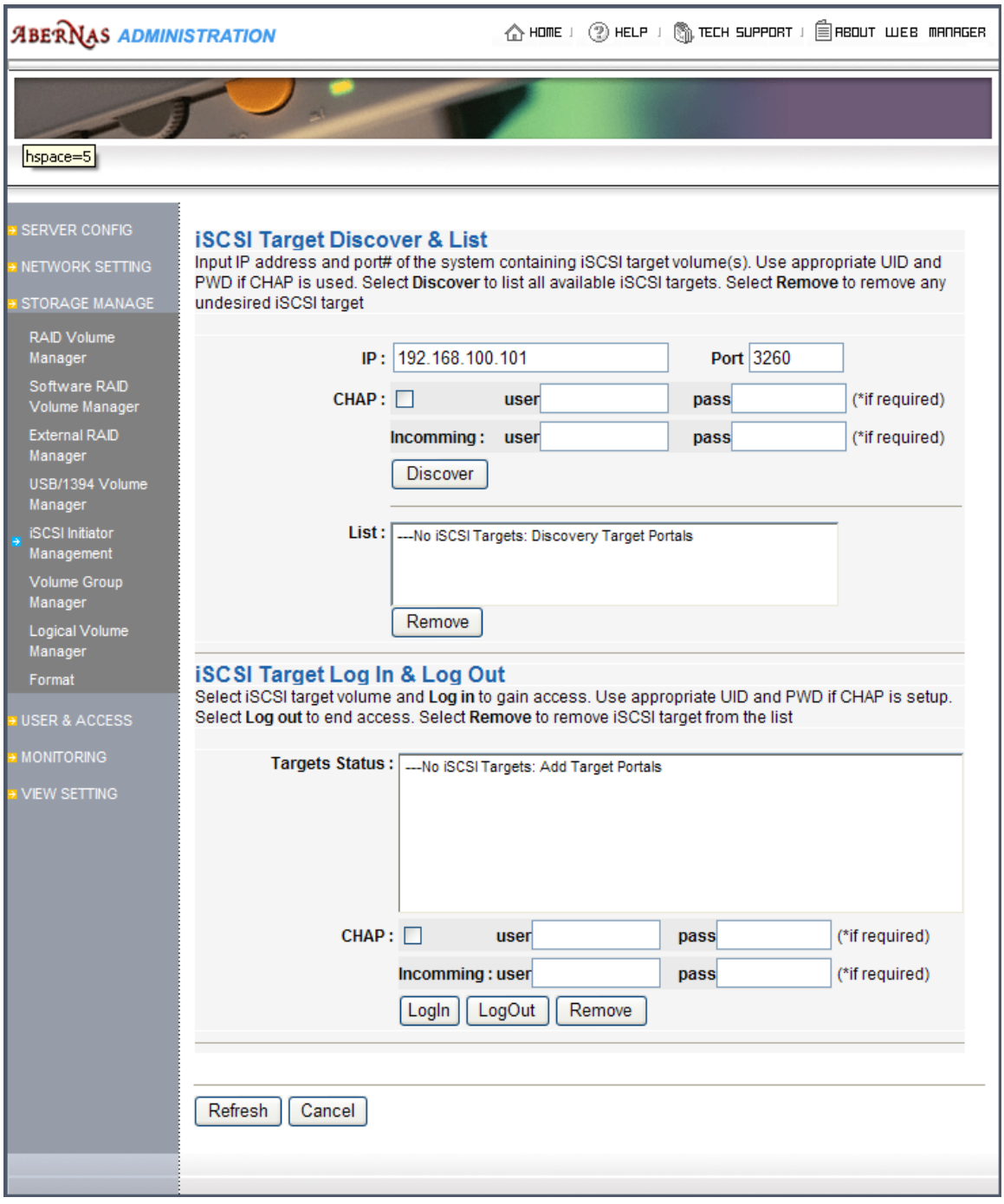
To Remove USB/1394 Volume:

1. Select USB/1394 Volume from **External Storage Volume Pool**
2. Select **Remove** button. Unfinished process to USB/1394 Volume may be interrupted.

Warning:

USB/1394 Volume is not intended to be used as part of a RAID Volume.
Do not remove USB/1394 Volume without selecting the Remove button, as it may result in unexpected failure.

Web Administration Interface > MANAGE > Storage Management – iSCSI Initiator Management



The iSCSI Initiator Manager connects the ABERNAS system to internal and external iSCSI target devices.

iSCSI Target Devices Benefits:

- Expand storage volume without having to add more disk drives to the ABERNAS.

- Ability to manage Logical Volumes residing both internally and externally to the ABERNAS system.
- Aggregate multiple iSCSI target devices into a single, large, storage space.
- No Fibre Channel or SCSI bus needed to connect to external storage subsystem.

Discover Available iSCSI Target Portals and iSCSI Target Devices:

1. Input **IP ADDRESS** and **PORT NUMBER** (3 60 is default) of the system that contains iSCSI target devices.
2. For iSCSI target devices that use Challenge Handshake Authentication Protocol (CHAP), enter the USER ID and PASSWORD for the OUTGOING and INCOMING fields. OUTGOING authenticates the ABERNAS system when it access remote iSCSI target device hosts. INCOMING authenticates remote iSCSI target device hosts when it connects to the ABERNAS iSCSI initiator systems.
3. Click on **DISCOVERY** and list of iSCSI target devices will displayed on the LIST field.
4. To remove an iSCSI target device, select it from the LIST and click **REMOVE**.

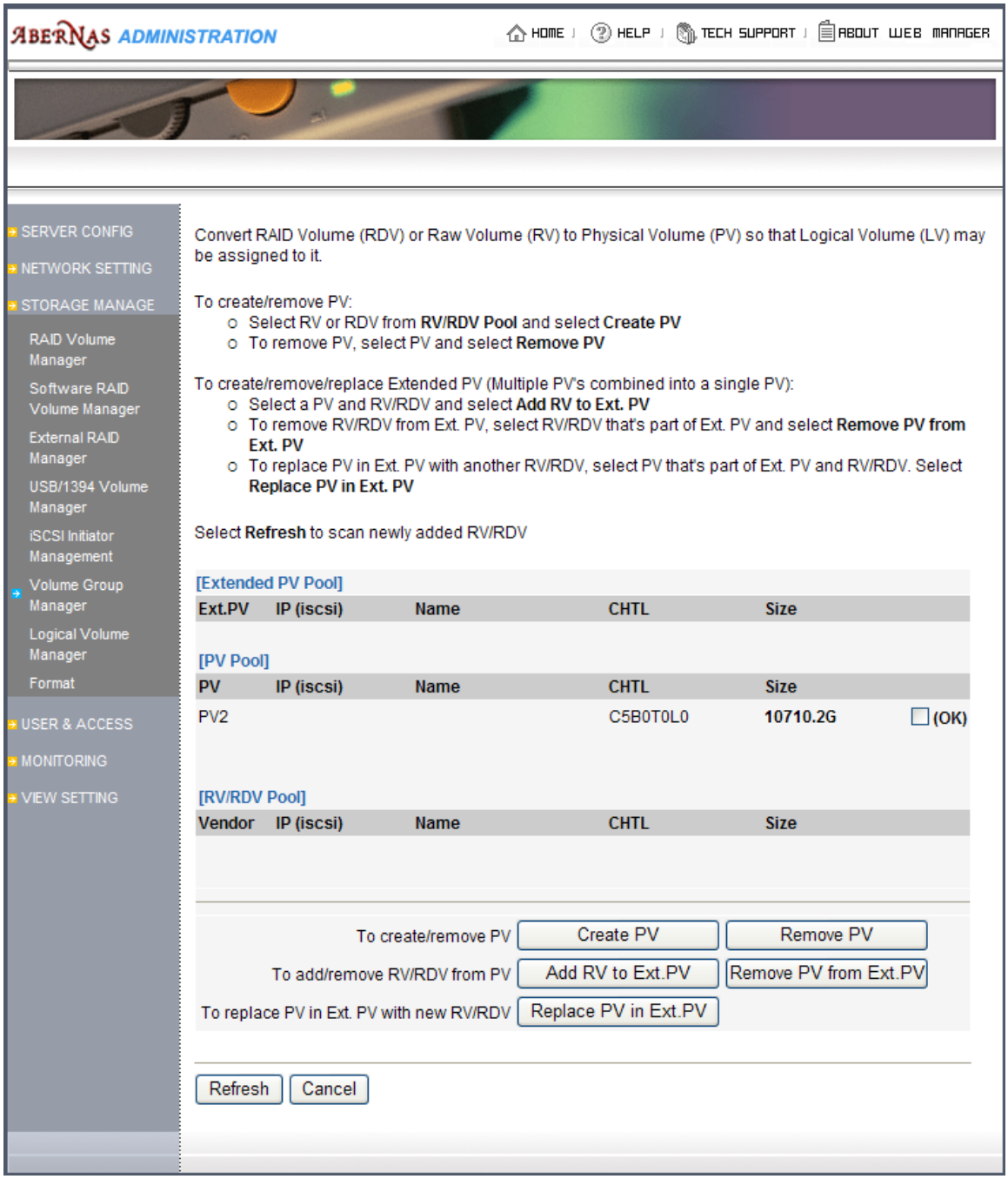
Connecting And disconnecting iSCSI Target devices:

1. Select desired iSCSI target device to connect
2. If selected iSCSI target devices use CHAP, then enter the OUTGOING and INCOMING USER ID and PASSWORD.
3. Click **LOG IN** button to connect, or to disconnect, select the desired iSCSI target device then click the **LOG OUT** button.

PV/RV Information:

This information lists the status of any detected iSCSI target devices. PV POOL shows connected iSCSI target devices that are part of Physical Volume list. RV POOL shows the available iSCSI target devices that have not been connected.

Web Administration Interface > MANAGE > Storage Management – Volume Group Manager


ABERNAS ADMINISTRATION
HOME | HELP | TECH SUPPORT | ABOUT WEB MANAGER
SERVER CONFIG
NETWORK SETTING
STORAGE MANAGE
RAID Volume Manager
Software RAID Volume Manager
External RAID Manager
USB/1394 Volume Manager
iSCSI Initiator Management
Volume Group Manager
Logical Volume Manager
Format
USER & ACCESS
MONITORING
VIEW SETTING
Convert RAID Volume (RDV) or Raw Volume (RV) to Physical Volume (PV) so that Logical Volume (LV) may be assigned to it.
To create/remove PV:
Select RV or RDV from RV/RDV Pool and select Create PV
To remove PV, select PV and select Remove PV
To create/remove/replace Extended PV (Multiple PV's combined into a single PV):
Select a PV and RV/RDV and select Add RV to Ext. PV
To remove RV/RDV from Ext. PV, select RV/RDV that's part of Ext. PV and select Remove PV from Ext. PV
To replace PV in Ext. PV with another RV/RDV, select PV that's part of Ext. PV and RV/RDV. Select Replace PV in Ext. PV
Select Refresh to scan newly added RV/RDV
[Extended PV Pool]
Ext.PV IP (iscsi) Name CHTL Size
[PV Pool]
PV IP (iscsi) Name CHTL Size
PV2 C5B0T0L0 10710.2G (OK)
[RV/RDV Pool]
Vendor IP (iscsi) Name CHTL Size
To create/remove PV
Create PV
Remove PV
To add/remove RV/RDV from PV
Add RV to Ext.PV
Remove PV from Ext.PV
To replace PV in Ext. PV with new RV/RDV
Replace PV in Ext.PV
Refresh
Cancel

Volume Group is comprised of Physical Volume (PV), Expanded Physical Volume (Exp. PV), and Raw Volume (RV). Volume Group Manager features:

- Convert RV to PV
- Add RV to PV, thus, creating Expanded PV
- Remove PV to RV Pool
- Remove or Replace RV that's been added to PV

Creating PV:

Creating PV is to convert the RV from the RV Pool to PV. Once RV is converted to PV, it is ready to be converted to Logical Volume (LV). Conversion from PV to LV means PV is formatted and ready to be used by clients attached to the ABERNAS.

To create PV, select the desired RV from the RV POOL and click **CREATE PV**.

Removing PV:

PVs in the PV POOL or EXPANDED PV POOL can be removed and converted into RV. To remove PV, select the desired PV from the PV POOL or EXTENDED PV POOL.

Adding RV to PV:

RV's in the RV POOL can be added to the PV in the PV POOL to expand the capacity of the original PV, or, insert more LVs.

To add the RV to the PV, select the desired available volumes from the PV POOL list, then click **ADD RV TO PV**.

This process adds RV to the existing PV, thus, creating the Expanded PV. The added RV is now named PV.

NOTE:

RV's that were iSCSI target devices or SCSI devices require manual conversion into LVs to be usable by the attached clients.

Separate The PV From Expanded PV:

To remove the PV that's been added to the PV, click on the PV from the EXPANDED PV POOL and click on **REMOVE PV FROM EXP. PV**.

This process removes the PV from the EXPANDED PV, converts the PV to RV and places it in the RV POOL as an RV. Physical Volume Expansion may be used to combine multiple PVs to create a single, large PV. This process can be useful when combining multiple PVs belonging to different RAID controller cards.

Replace The PV In the Expanded PV with Another RV:

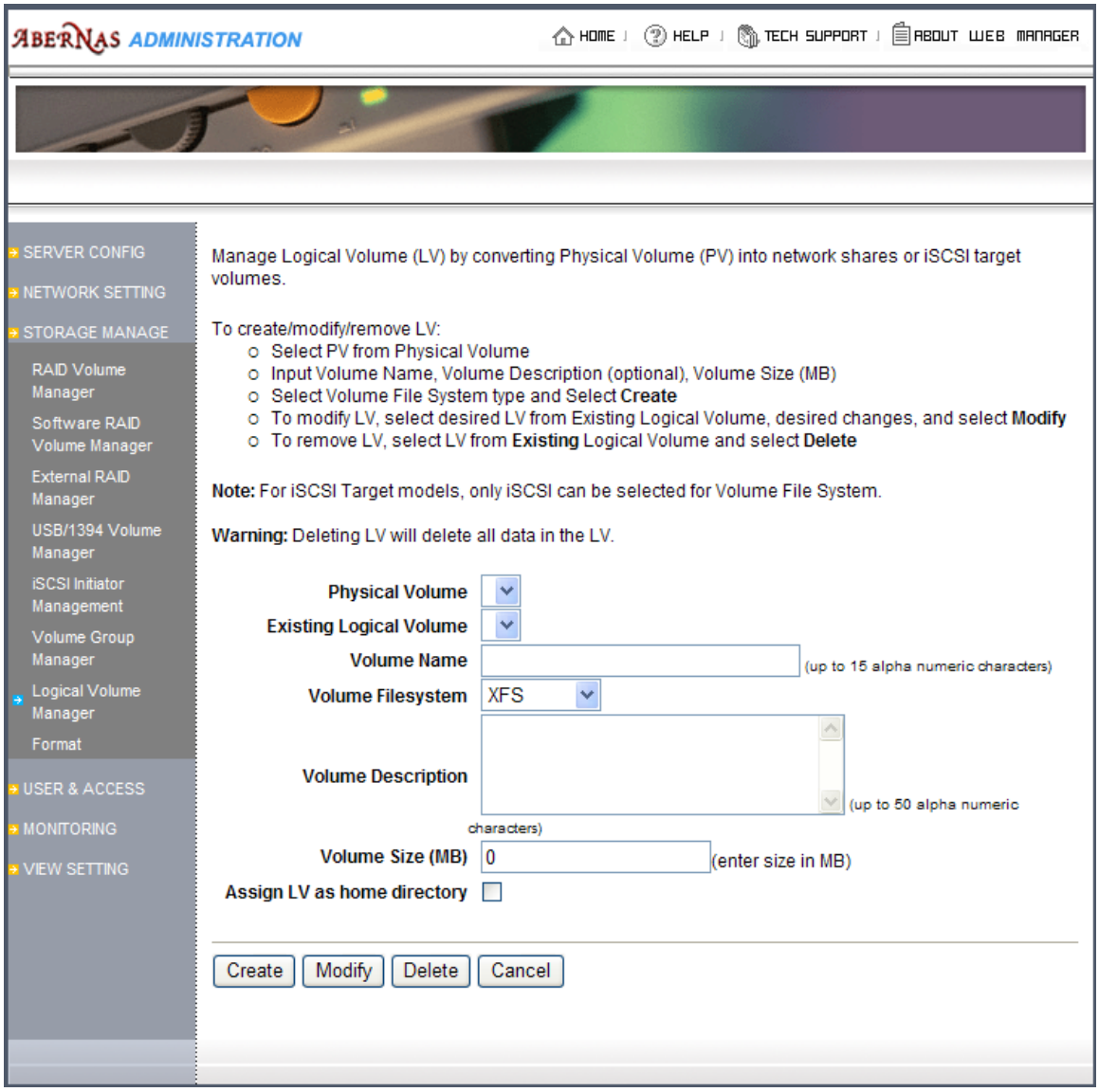
To replace a PV belonging to an Expanded PV with another RV, all necessary volumes can be selected at once rather than removing first, then, adding next.

Select the PV belonging to EXPANDED PV, select the RV you wish to replace the PV selected, click on **REPLACE PV IN EXP. PV** or click **CANCEL** to discard the changes and return to the Administration Home Page.

CAUTION:

Removing PV, separating PV, or replacing PV will cause the PV to loose its data.

Web Administration Interface > MANAGE > Storage Management – Logical Volume Manager


ABERNAS ADMINISTRATION
HOME | HELP | TECH SUPPORT | ABOUT WEB MANAGER
SERVER CONFIG
NETWORK SETTING
STORAGE MANAGE
RAID Volume Manager
Software RAID Volume Manager
External RAID Manager
USB/1394 Volume Manager
iSCSI Initiator Management
Volume Group Manager
Logical Volume Manager
Format
USER & ACCESS
MONITORING
VIEW SETTING
Manage Logical Volume (LV) by converting Physical Volume (PV) into network shares or iSCSI target volumes.
To create/modify/remove LV:
Select PV from Physical Volume
Input Volume Name, Volume Description (optional), Volume Size (MB)
Select Volume File System type and Select Create
To modify LV, select desired LV from Existing Logical Volume, desired changes, and select Modify
To remove LV, select LV from Existing Logical Volume and select Delete
Note: For iSCSI Target models, only iSCSI can be selected for Volume File System.
Warning: Deleting LV will delete all data in the LV.
Physical Volume
Existing Logical Volume
Volume Name
(up to 15 alpha numeric characters)
Volume Filesystem
XFS
Volume Description
(up to 50 alpha numeric characters)
Volume Size (MB)
0
(enter size in MB)
Assign LV as home directory
Create
Modify
Delete
Cancel

A Logical Volume (LV) is a formatted storage volume in PV that can be shared by network clients attached to the AberNAS. By default, all users are given access to a logical volume. To assign exclusive access to specific users or user groups, go to the User and Access section.

Functions of Logical Volume Manager Are:

- Create Logical Volume
- Designate file system or iSCSI to Logical Volume
- Modify Logical Volume
- Delete Logical Volume

NOTE:

The Reiser File System has superior performance when working with smaller size files, such as database files. The XFS file system has superior performance when working with large size files, such as video. LV size cannot be decreased in XFS. In order to decrease the size of the LV, it must first be deleted and then recreated. XFS LVs can be increased in size without deleting the volume.

Creating a New Logical Volume:

1. Select a Physical Volume with available space from the PHYSICAL VOLUME pull down menu.

NOTE:

Do not use identical names for logical Volumes, even if they belong to different physical Volumes.

2. Enter a unique name in the VOLUME NAME field. Names can be up to 15 alphanumeric characters and must not contain spaces.
3. If it is beneficial to add a description of this Logical Volume to help identify its use, enter that description in the VOLUME DESCRIPTION field using up to 50 alphanumeric characters. This is an optional field.
4. Enter the storage size of the Logical Volume in Megabytes in the VOLUME SIZE field, keeping in mind the amount of available space.
5. Select a file system for the Logical Volume from the VOLUME FILESYSTEM pull down menu. Reiser FS and XFS support network clients such as Microsoft, UNIX/Linux, and Apple. iSCSI is a network based block device connected through SCSI over IP protocol, formatted and used as a network storage volume.
6. Click on **CREATE** to complete the configuration of this Logical Volume or click **CANCEL** to discard the changes and return to the Administration Home Page. Repeat the above steps to create and configure additional logical volumes.

Modify an Existing Logical Volume:

1. Select the Physical Volume containing the Logical Volume to modify from the PHYSICAL VOLUME pull down menu. The Logical Volume(s) contained in the selected Physical Volume will populate in the EXISTING LOGICAL VOLUME pull down menu.
2. Select the Logical Volume to modify from the EXISTING LOGICAL VOLUME pull down menu. The current Logical Volume information is immediately displayed on the screen.
3. Modify the VOLUME NAME, VOLUME DESCRIPTION, VOLUME TYPE and/or VOLUME SIZE as needed.

CAUTION:

Changing the VOLUME FILE SYSTEM type will delete all data on the device.

4. To complete the modification, click on **MODIFY** or click **CANCEL** to discard the changes and return to the Administration Home Page.

NOTE:

Size cannot be modified if snapshot Volume is attached to the logical Volume.

Delete a Logical Volume:

1. Select the Physical Volume that contains the Logical Volume you wish to delete from the PHYSICAL VOLUME pull down menu. A list of Logical Volumes for the selected Physical Volume appears in the EXISTING LOGICAL VOLUME pull down menu.
2. Select the Logical Volume to delete from the EXISTING LOGICAL VOLUME pull down menu.

CAUTION:

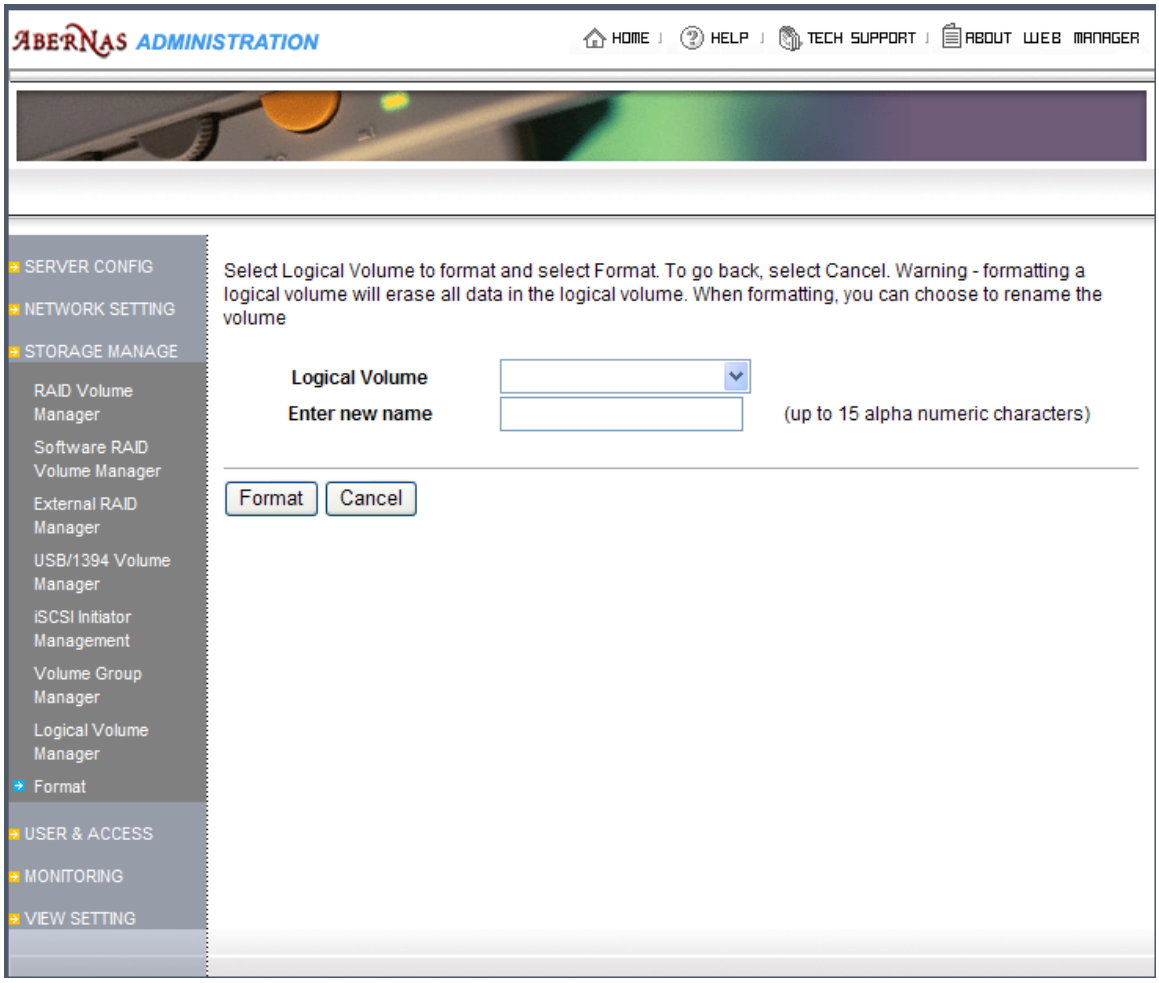
Deleting logical Volumes cannot be undone and data will be lost. Be sure to select the correct logical Volume. If snapshot Volume is associated with the selected logical Volume, snapshot Volume must be deleted first.

3. Click **DELETE** at the bottom of the page. The selected Logical Volume is removed from the Select Logical Volume list or click **CANCEL** to discard the changes and return to the Administration Home Page.

NOTE:

Logical Volume cannot be deleted if snapshot Volume is attached to the logical Volume.

Web Administration Interface > MANAGE > Storage Management – Format



Format a logical volume to erase all of its contents. Although it is not required, you can also change the logical volume name.

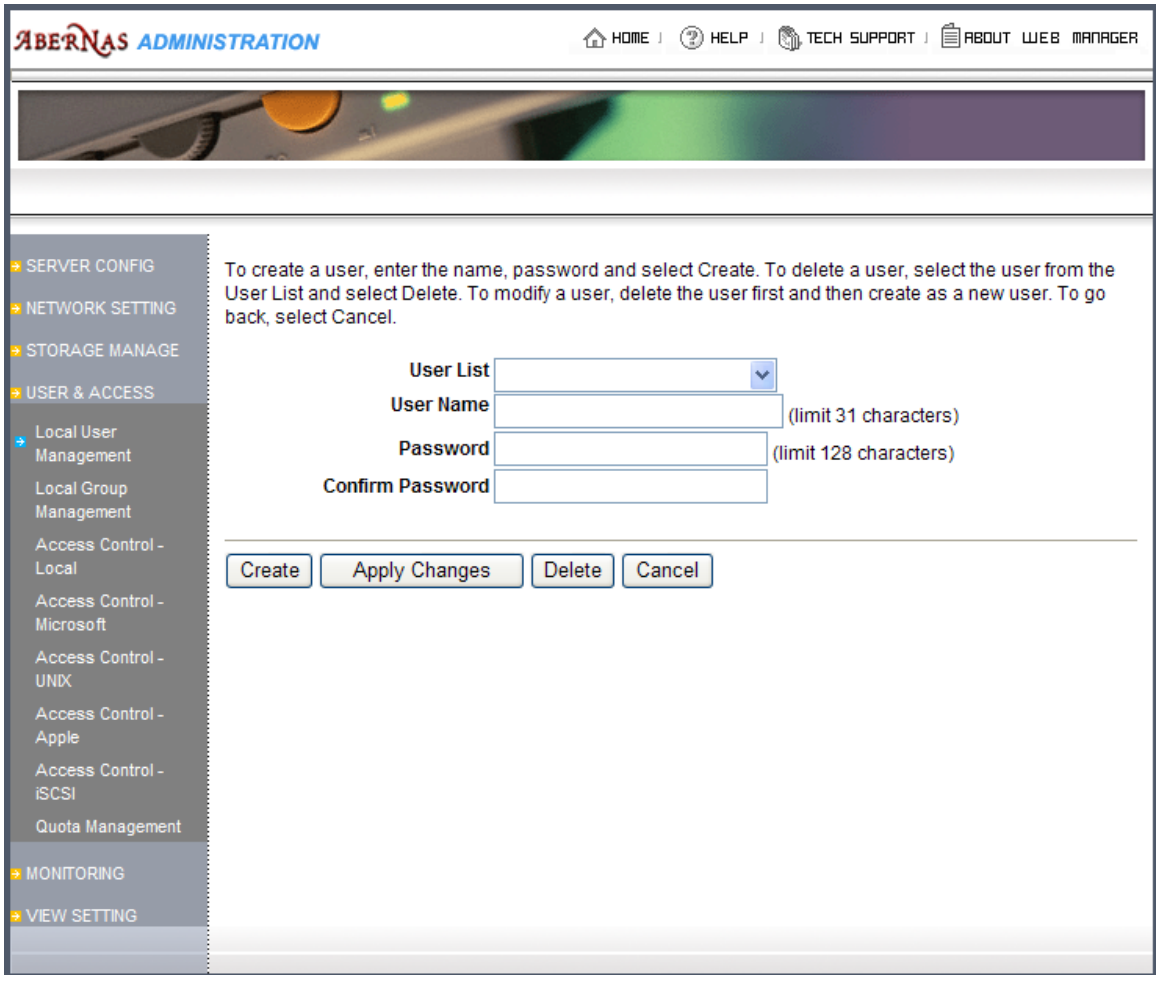
CAUTION:

Formatting a physical volume cannot be undone and you will be asked to confirm your request. Be sure to move data you need to save to another location before formatting the volume.

Format a Logical Volume:

1. Select the logical volume from the LOGICAL VOLUME pull down menu.
2. To change the VOLUME NAME (optional), enter the new name in the ENTER NEW NAME field. Names can be up to 15 alphanumeric characters and must not contain spaces.
3. Click on **FORMAT**. The AberNAS immediately begins to format the selected logical volume. Click **CANCEL** to discard the changes and return to the Administration Home Page.

Web Administration Interface > MANAGE > User & Access – Local User Management



Local users are those user accounts that are created within the AberNAS specifically for access to the AberNAS files and folders. Once local users are created, they can be assigned to logical volumes as individual users or as part of a user group.

Create Local Users:

1. Enter the user name with a maximum of 5 characters in the USER NAME field.
2. Enter a unique password in the PASSWORD fields - between 6-8 alphanumeric characters without spaces. The password is case-sensitive.
3. Click **CREATE** to add the user to the local user list or click **CANCEL** to discard the changes and return to the Administration Home Page. Repeat the steps above to create additional local users.

NOTE:

The AberNAS seeks and lists users and groups in local, LDAP, NIS, and ADS/PDC. Duplicate user IDs and groups will also be listed in this order: local, LDAP, NIS, and ADS/PDC.

Access a User's Home directory:

A Home directory is a private directory that is a designated for a user. This user has the highest level of access control to this directory designated by the Administrator/Owner. Home directory can be accessed by using two methods:

1. Map to the Logical Volume Share that contains the user home directory.
2. Access via Web browser by entering ftp://user_name@server.com or IP address of the server.

Delete a User From The Local Users' List:

1. Select the user to delete from the USER LIST.
2. Click **DELETE** to complete this process or click **CANCEL** to discard the changes and return to the Administration Home Page.

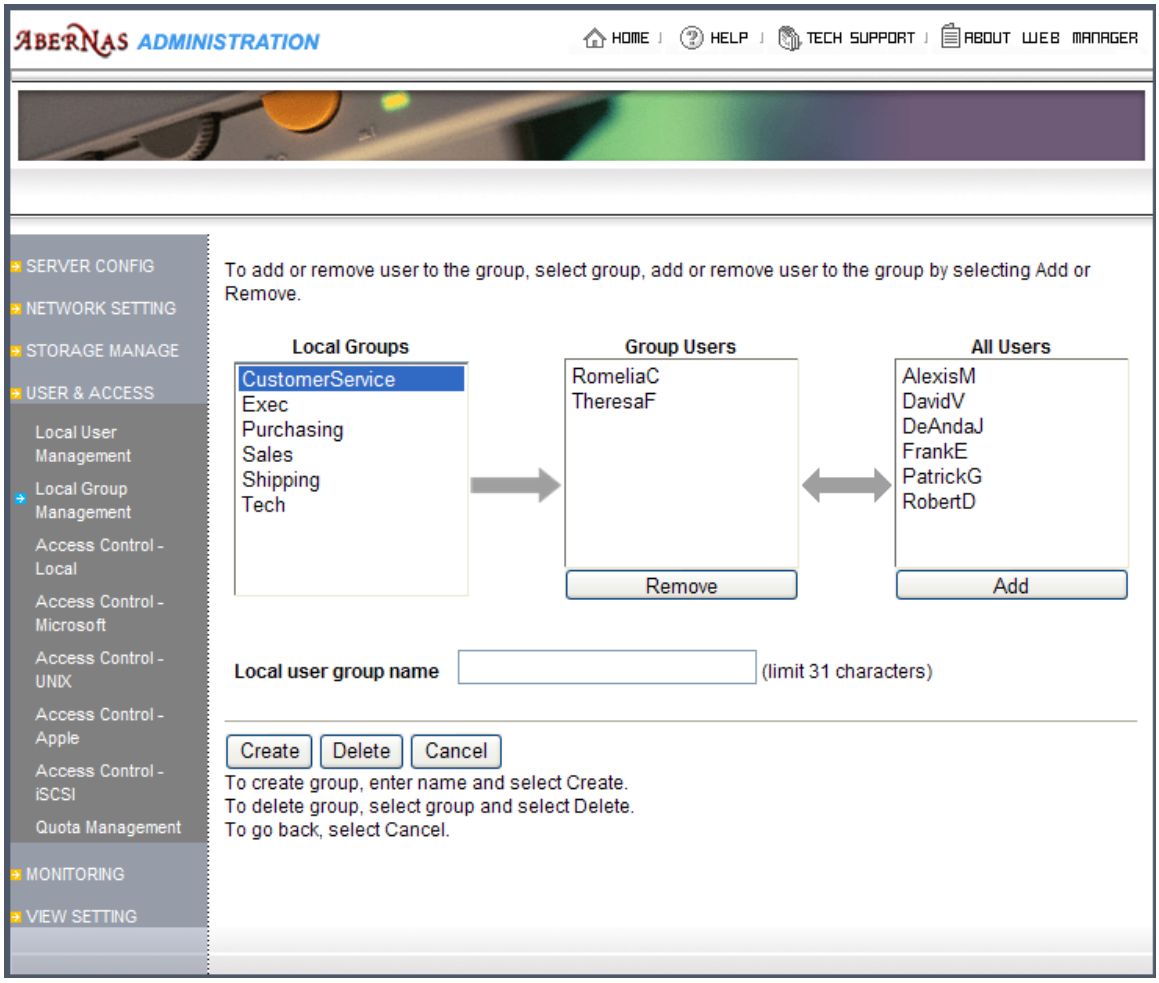
CAUTION:

Deleting users cannot be undone and you will be asked to confirm deletion. Be sure to select the correct user(s).

Modify an Existing User:

1. Select the user from the USER LIST.
2. Enter the new information in the appropriate fields.
3. Click **APPLY CHANGES** to complete this process or click **CANCEL** to discard the changes and return to the Administration Home Page.

Web Administration Interface > MANAGE > User & Access – Local Group Management



User groups are formed to easily manage a group of users and apply access levels to the entire group for specific logical volumes. The new user groups you create will be available to assign to logical volumes on the Microsoft and Apple Access Control Pages.

Create Local User Groups:

1. Enter a unique name for the user group in the LOCAL USER GROUP NAME field, up to a maximum of 15 alphanumeric characters.
2. Click **CREATE**. The new local user group will appear in the LOCAL GROUPS list or click **CANCEL** to discard the changes and return to the Administration Home Page.

Add User To User Groups:

1. Select the group from the LOCAL GROUPS list.
2. Select the user from the ALL USERS list and click **ADD**. Multiple users can be selected using the CTRL and SHIFT keys.

NOTE:

The AberNAS seeks and lists users and groups in local, LDAP, NIS, and ADS/PDC. In the event where you have duplicate user IDs, the above order will be used to list and accept duplicate users and groups.

Modify/delete Local User Groups:

1. Select the user group to modify from the LOCAL GROUPS list. The members of the user group are immediately displayed in the GROUP USERS list.
2. Add a user by selecting the user from the ALL USERS list and clicking on **ADD** or Delete a user by selecting the user from the GROUP USERS list and click **REMOVE.**
3. Repeat the steps above until you have modified all necessary user groups.

NOTE:

To change the name of the user group, you must delete the existing user group and re-create with the desired name.

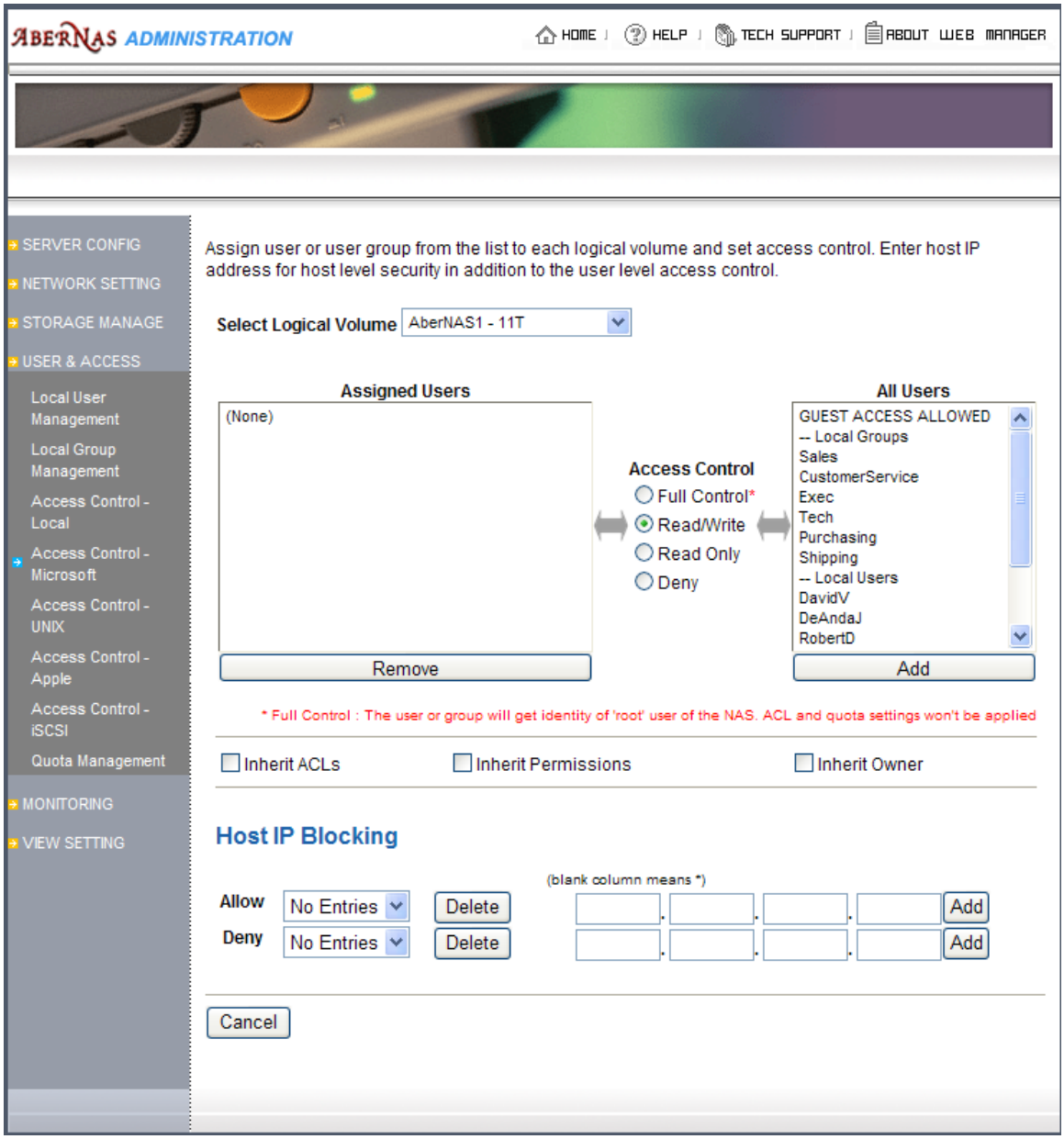
Delete a User Group:

1. Select the user group to delete from the LOCAL GROUPS list.
2. Click **DELETE**. The selected user group is removed from the LOCAL GROUPS list. Click **CANCEL** to discard the changes and return to the Administration Home Page.

CAUTION:

Deleting user groups cannot be undone and you will be asked to confirm deletion. Be sure to select the correct user group(s).

Web Administration Interface > MANAGE > User & Access – Access Control – Microsoft



Once logical volumes have been created, users or user groups can be assigned to have access to specific logical volumes. By default, all users are given access to a new logical volume. You can assign exclusive access rights to a logical volume to one user group or to individual users. Furthermore, you can specify an individual user, who is part of a user group, to have higher or lower access level than the rest of the group. This section controls the access control at the directory level. For sub-directory and file level access control, user must assign them directly to the sub-directory, or file, from the Microsoft client.

Assign Access Control:

To assign users and/or user groups access to a logical volume, follow the steps below:

1. Select the logical volume that you wish to give user access to from the SELECT LOGICAL VOLUME pull down menu.
2. Select the user(s) and/or user group(s) from the ALL USERS list.
3. Select FULL CONTROL, READ/WRITE, READ ONLY or DENY from the ACCESS CONTROL radio button list for setting the access levels:

- FULL CONTROL – Read, write, and delete file privileges to the selected logical volume
- READ/WRITE – Read and write files to the selected logical volume. Users will not be able to delete files.
- READ ONLY – Read privileges to the selected logical volume. Users will not be able to add new files, modify files or delete files.
- DENY – All access is denied to the selected logical volume for the user. This is necessary when you wish to give access to a user group except for an individual user within that group. Any individual user within a user group can be assigned with different access level from the rest of the user group by assigning a different access level to the individual user for the logical volume. The individual user access level takes priority over the user group access level. User will not be able to read, write or delete any files within the logical volume.

4. Click on **ADD**.
5. To remove a user or user group from the logical volume, select them from the ASSIGNED USERS list and click **REMOVE**.
6. Add or delete additional user(s) and/or user group(s) to the logical volume by repeating steps 1 through 5 above.

Host IP Blocking:

In addition to user level access control, you can specify host-level security by adding the host IP addresses to the ALLOW or DENY host IP blocking lists.

Add IP Address to Allow or Deny List:

1. Select the logical volume that you wish to assign host IP blocking from the SELECT LOGICAL VOLUME pull down menu.
2. Enter the IP address of the host in the appropriate ALLOW or DENY fields then click **ADD** to add the IP address to the respective list. Click **CANCEL** to discard the changes and return to the Administration Home Page.

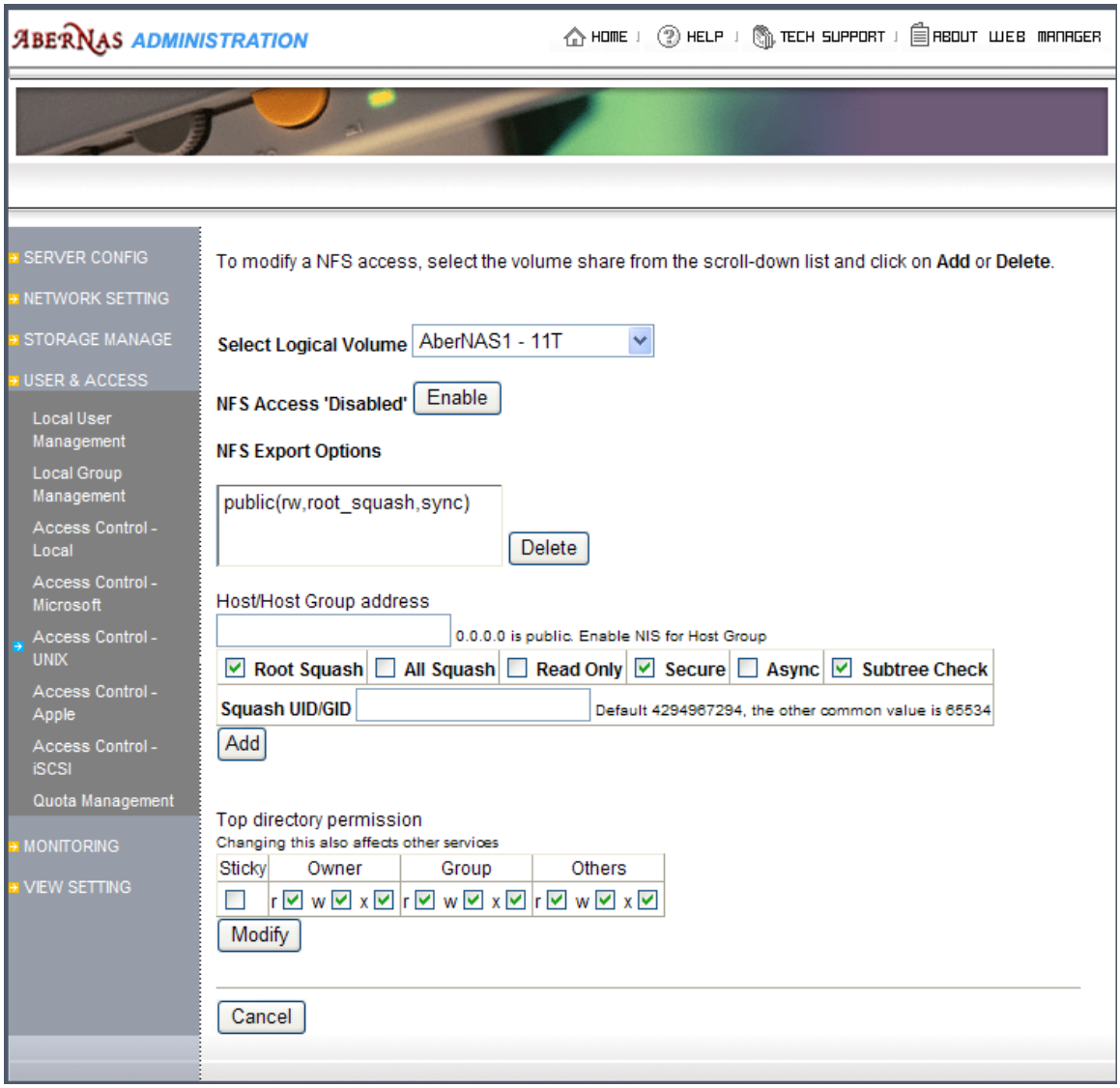
Delete an IP Address to Allow or Deny List:

1. Select the logical volume where you wish to assign host IP blocking from the SELECT LOGICAL VOLUME pull down menu.
2. Select the IP address from the ALLOW or DENY pull down menu, then click **DELETE** to remove the IP Address from the respective list. Click **CANCEL** to discard the changes and return to the Administration Home Page.

NOTE:

When an IP address is added to the Allow List, those on the Allow List are the only host IP addresses that will be allowed to access the logical Volume. When an IP address is added to the Deny List, those on the Deny list are the only host IP addresses that will be denied from accessing the logical Volume.

Web Administration Interface > MANAGE > User & Access – Access Control – UNIX



NOTE:

Synchronizing the AberNAS with NIS does not automatically give NIS users access to the logical Volume. All Logical Volumes to be accessed by NIS users must first be mounted by the host computer.

Add Host Access:

1. Select the logical volume that you wish to give host access to from the SELECT LOGICAL VOLUME pull down menu.
2. Click **Enable** NFS Access.

NOTE:

Selecting Enable NFS SERVICE from the Network Settings Interface of the web administration GUI enables global NFS access. Disabling this option disables NFS access completely. Unless NFS access is added with host IP address for each logical volume, NFS access for that logical volume is disabled. As a result, the pull down menu of the NFS access for the logical volume share is disabled by default.

3. Type in the IP address of the UNIX host in the HOST IP ADDRESS field and select the desired mounting options for this host.

Up to four access levels may be applied to each host that is added to the logical volume:

- ROOT SQUASH – Any user logging in as "root" will be assigned a different user ID so that limited privilege of read/write/delete is assigned to the logged-in user.
- ALL SQUASH – Any user logging in will be assigned a different user ID so that limited privilege of read/write/delete is assigned to the logged in user.
- READ ONLY – Any user logging in can have read-only access.
- SECURE – Secure option limits the user that can mount to NFS file system to super users only (TCP/IP port #10 4 and below). If a third party application exists that allows non-super users to mount to the NFS file system, secure option should be deselected.
- ASYNC – Allows the NFS server to violate the NFS protocol and reply to requests before any changes made by that request have been committed to stable storage (e.g. disc drive). Using this option usually improves performance, but at the cost that an unclean server restart (i.e. a crash) can cause data to be lost or corrupted.
- SUBTREE CHECK – If a subdirectory of a file system is exported, but the whole file system isn't then whenever an NFS request arrives, the server must check not only that the accessed file is in the appropriate file system but also that it is in the exported tree. By default, top directory permission is set to rwx/rwx/rwx. To modify, select the desired rwx permission settings for OWNER, GROUP and OTHER from the TOP DIRECTORY PERMISSION check boxes.

STICKY BIT – When Sticky bit is enabled on a directory, files inside the directory may be renamed or removed only by the owner of the file, the owner of the directory, or the super user (even if the modes of the directory would otherwise allow such an operation).

3. Click **MODIFY** to complete or click **CANCEL** to discard the changes and return to the Administration Home Page.

NOTE:

STICKY BIT is used to allow only the root or the owner of the file to unlink or rename the file. When disabled, anyone that has access to the directory can rename or unlink the file.

Delete The Host:

1. Select the IP address from the IP ADDRESS pull down menu.
2. Click **DELETE** or click **CANCEL** to discard the changes and return to the Administration Home Page.

NOTE:

Each IP address must be deleted manually. Changing the logical volume share and setting it to DISABLE does NOT delete IP address(es).

Security Method for NFS Access:

The AberNAS implements standard UNIX security for NFS access. This means that the UNIX host that is added to the logical volume can mount to the logical volume with assigned access privileges. Any user logging into the host is authenticated by the NIS (Network Information Service) server or the UNIX host's own security.

After the user is logged into the host, he/she is able to access the logical volume on the ABERNAS with read/write/delete or read-only privilege, depending on the access privilege that

was assigned to the host. Individual subdirectories created by the user can be secured by applying one of the following:

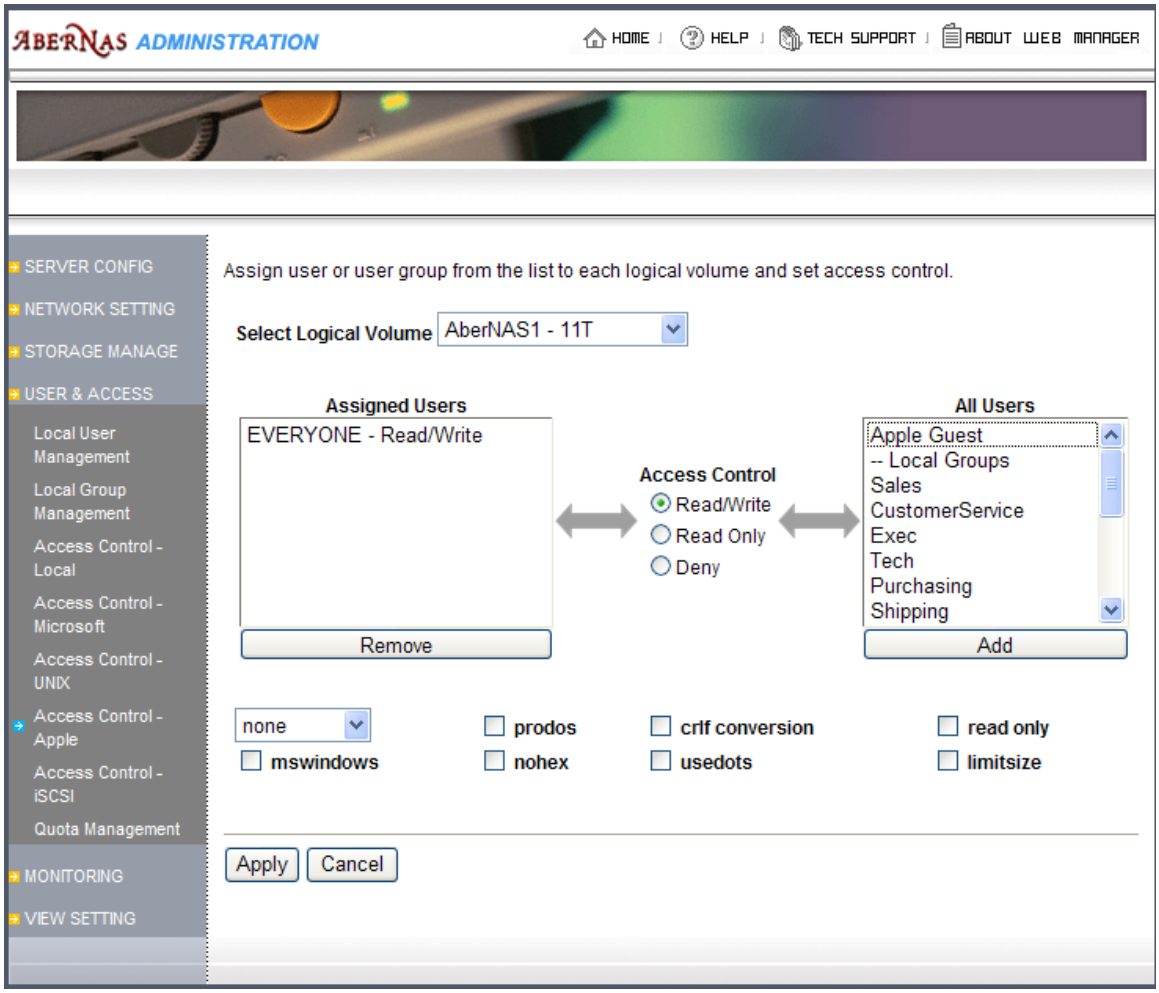
1. OWNER ONLY
2. USER GROUP THAT THE USER BELONGS TO
3. EVERYONE IN THE SUB-DIRECTORY.

Mounting Syntax:

ABERNAS shares are mounted under the /exports directory. Sample mounting syntax is as below:

mount -t nfs 10.1.1.201:/exports/share0 /host local directory

Web Administration Interface > MANAGE > User & Access – Access Control – Apple



Once logical volumes have been created, local or NIS, users or user groups can be assigned to have access to specific logical volumes. By default, all users are given access to a new logical volume. You can assign exclusive access rights to a logical volume to one individual user or one entire user group. Furthermore, you can specify an individual user, who is part of a user group, to have higher or lower access level than the rest of the group. This section controls the access control at the directory level. For sub-directory and file level access control, user must assign them directly to the sub-directory or file, from the host.

Assign Access Control:

To assign users and/or user groups access to a logical volume, follow the steps below:

1. Select the logical volume that you wish to give user access to from the SELECT LOGICAL VOLUME pull down menu.
2. Select the users and/or user groups from the ALL USERS list.
3. Select FULL CONTROL, READ/WRITE, READ ONLY or DENY from the ACCESS CONTROL radio button list for setting the access levels:

- READ/WRITE – Read and write files to the selected logical volume. Users will not be able to delete files.

- READ ONLY – Read privileges to the selected logical volume. Users will not be able to add new files, modify files or delete files.
- DENY – All access is denied to the selected logical volume for the user. This is necessary when you wish to give access to a user group except for an individual user within that group. Any individual user within a user group can be assigned with different access level from the rest of the user group by assigning a different access level to the individual user for the logical volume. The individual user access level takes priority over the user group access level. User will not be able to read, write or delete any files within the logical volume.

4. Click **ADD** to complete this process.
5. To remove a user or user group from the logical volume, select them from the ASSIGNED USERS list and click **REMOVE**.
6. To ADD or DELETE additional user(s) and/or user group(s) to the logical volume repeat all of the steps shown above.
7. Apply the following options if necessary by selecting their respective fields:

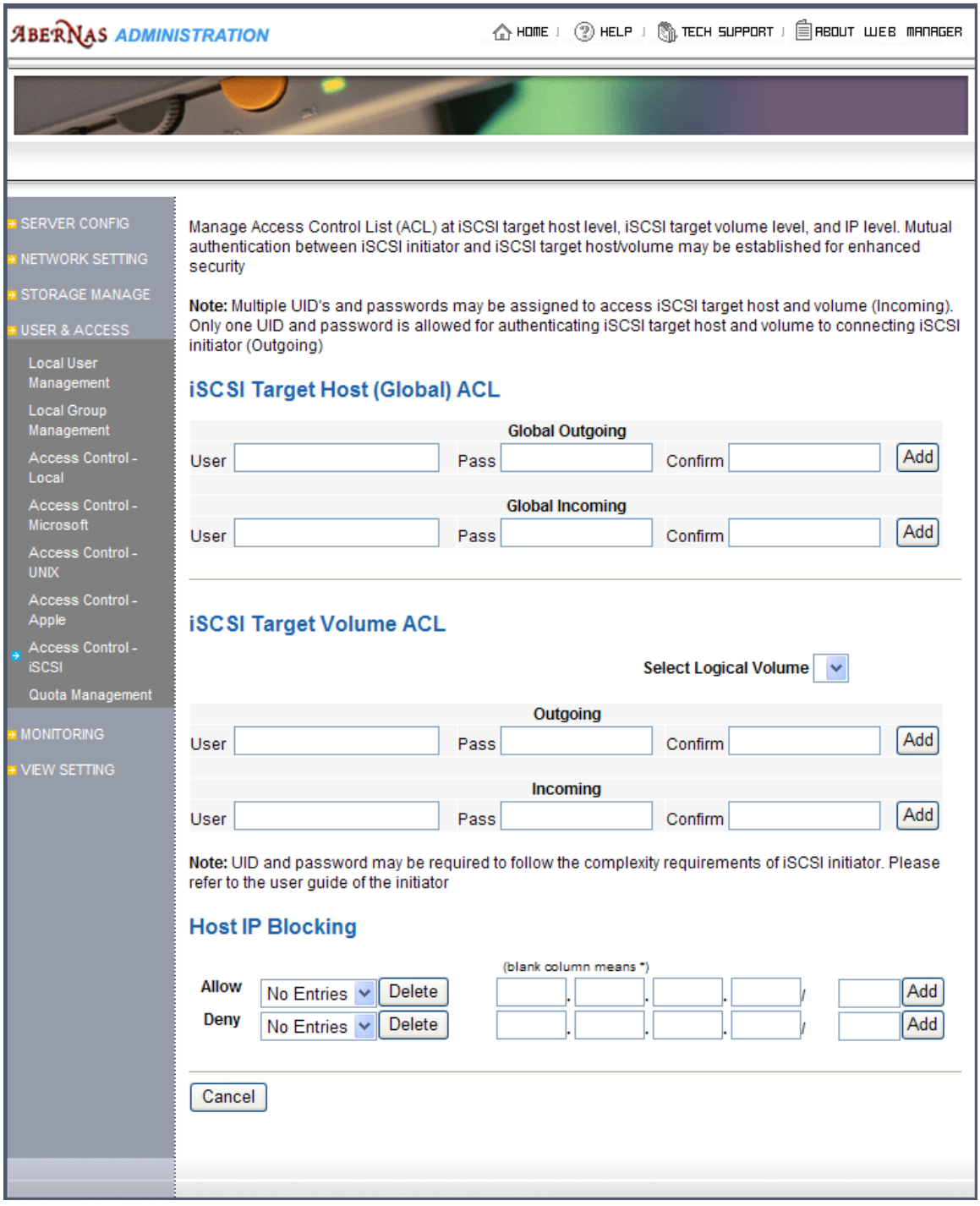
- casefold option: Casefold option handles how case names should be managed.
- tolower: Lower cases names in both directions.
- toupper: Upper cases names in both directions.
- xlatelower: Client sees lower case, server sees upper case.
- Xlateupper: Client sees upper case, server sees lower case.
- mswindows: Forces filename restrictions imposed by MS WinXX and invokes the MS default codepage (iso8859-1) if one is not already specified.
- prodos: Provides compatibility with Apple II clients.
- nohex: Disables hex.
- crlf conversion: Enables crlf translation for TEXT files.
- usedots: Don't do hex translation for dot files. This makes all files such as .Parent, .Apple* illegal. Dot files created on the server side will be invisible to the client.
- read only: Specifies the share as being read only for all users.
- limitsize: Hack for older Macintosh using newer Appleshare clients to limit the disk size reporting to GB.

8. Click **APPLY** to complete this process or click **CANCEL** to discard the changes and return to the Administration Home Page.

Restart AFP Service:

1. Click **RESTART SERVICE** to restart the AFP service.

Web Administration Interface > MANAGE > User & Access – Access Control – iSCSI



User and Access control can be applied to iSCSI target devices with User ID & Password as well as by Host IP of the client.

Global Users - Define the access control for all iSCSI target devices within the ABERNAS system. Having access as a global user allows this user to scan and view all iSCSI target devices in the system.

Target Users - Define the access control for individual iSCSI target devices. Each target device may have a different user ID and password, thus, the user may not have access to all of the target devices in the system.

Host IP Blocking - Controls access to each iSCSI target device by allowing or disallowing Host IP addresses of the client. This feature is a subset of Target Users, thus, each iSCSI target device must have its own HOST IP BLOCKING list.

Global and Target User(s):

There are two ways to control access at the user level:

1. **INCOMING:** Incoming user and password controls any users that are trying to access the iSCSI target device from another host in the network. This is the case for both Global Users and Target Users.

2. **OUTGOING:** Outgoing user and password controls the authenticity of iSCSI target device to the inquiring user. This is to certify to the incoming user that the system that they're trying to access is indeed the system they've intended to access.

NOTE:
This feature is not supported by all iSCSI initiators. Please refer to your iSCSI initiator manual for details.

NOTE:
Only 1 user ID and password is used for Outgoing user.

INCOMING and OUTGOING user(s) can apply to both Global User and Target User.

Creating a Global User:

1. Enter the user name and password in the USER NAME and PASSWORD fields.
2. CONFIRM PASSWORD.
3. Click **ADD** to create the user and add user name to the USER LIST . Same steps apply to both Incoming and Outgoing Users.

Creating a Target User:

1. Select LV from the SELECT LOGICAL VOLUME pull down menu.
2. Input user name and password in the USER NAME and PASSWORD fields.

NOTE:
Length of the password and character requirements depend on the iSCSI Initiator used. Refer to your iSCSI Initiator manual for details.

3. Confirm the password.
4. Click **ADD**. This will create the user and add the user to the USER LIST. Same steps apply to both Incoming and Outgoing Users.

NOTE:
The user list for iSCSI target devices, both Global and Target, is separate from the user list that belongs to local, NIS and ADS/PDC.

Delete User:

Select the desired user from the USER LIST and click the respective **DELETE** button. This applies to any user, Global or Target, Incoming or Outgoing.

Host IP Blocking:

In addition to user level access control, you can specify host-level security by adding the host IP address to the ALLOW or DENY host IP blocking lists.

Add IP Address to Allow or Deny List:

1. Select the logical volume that you wish to assign host IP blocking from the SELECT LOGICAL VOLUME pull down menu.
2. Enter the IP address and access port number (3260 is default) of the host in appropriate ALLOW or DENY fields then click **ADD** to add the IP address to the respective list. Click **CANCEL** to discard the changes and return to the Administration Home Page.

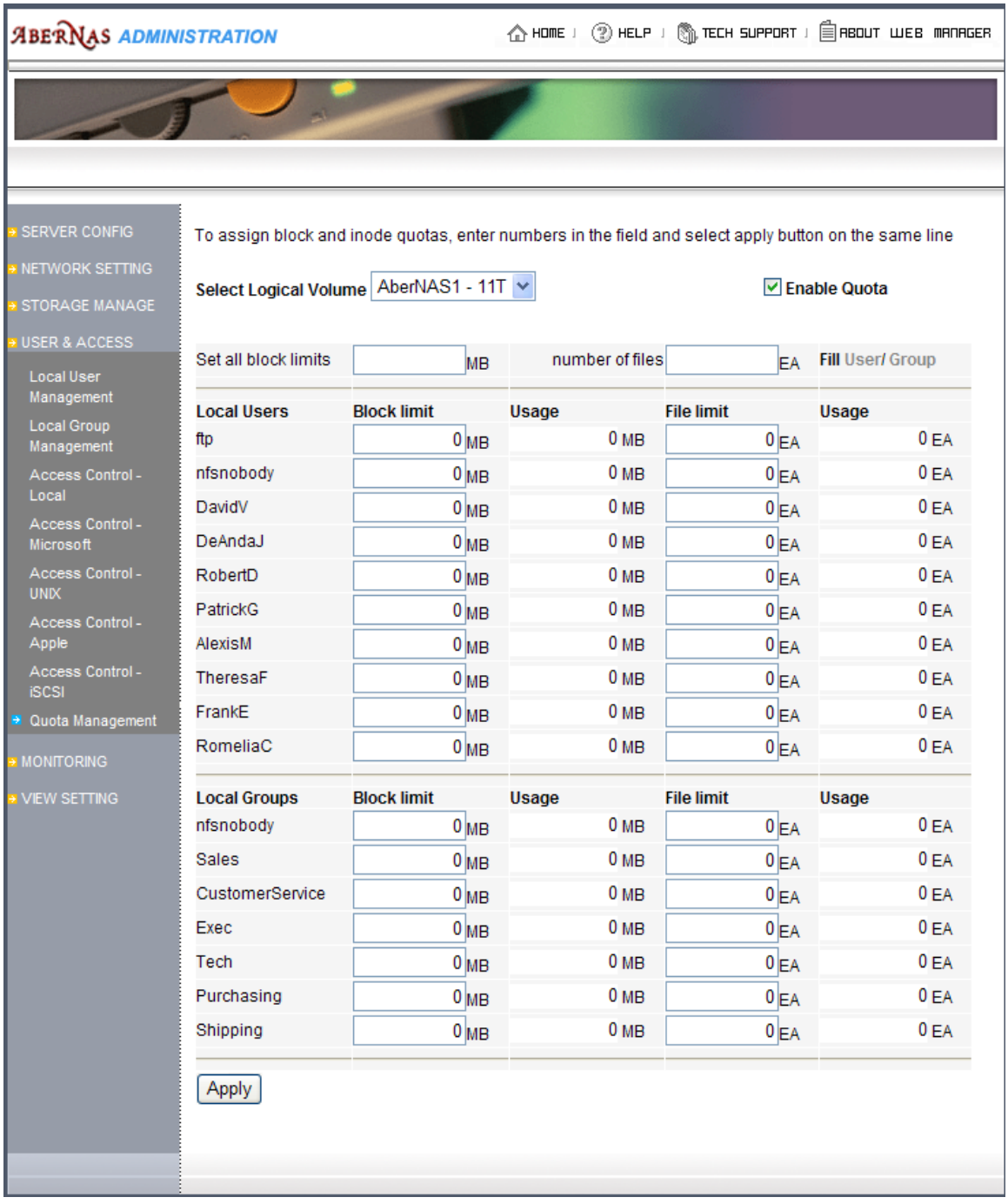
Delete an IP Address to Allow or Deny List:

1. Select the logical volume where you wish to assign host IP blocking from the SELECT LOGICAL VOLUME pull down menu.
2. Enter the IP address and access port number (3260 is default) of the host in appropriate ALLOW or DENY fields then click **DELETE** to add the IP address to the respective list. Click **CANCEL** to discard the changes and return to the Administration Home.

NOTE:

When an IP address is added to the allow list, those on the allow list are the only host IP addresses that will be allowed to access the target. When the IP address is added to the Deny List, those on the Deny List are the only host IP addresses that will be denied access the target.

Web Administration Interface > MANAGE > User & Access – Quota Management


ABERNAS ADMINISTRATION
HOME | HELP | TECH SUPPORT | ABOUT WEB MANAGER
SERVER CONFIG
NETWORK SETTING
STORAGE MANAGE
USER & ACCESS
Local User Management
Local Group Management
Access Control - Local
Access Control - Microsoft
Access Control - UNIX
Access Control - Apple
Access Control - iSCSI
Quota Management
MONITORING
VIEW SETTING
To assign block and inode quotas, enter numbers in the field and select apply button on the same line
Select Logical Volume AberNAS1 - 11T
Enable Quota
Set all block limits MB number of files EA Fill User/ Group
Local Users Block limit Usage File limit Usage
ftp 0 MB 0 MB 0 EA 0 EA
nfsnobody 0 MB 0 MB 0 EA 0 EA
DavidV 0 MB 0 MB 0 EA 0 EA
DeAndaJ 0 MB 0 MB 0 EA 0 EA
RobertD 0 MB 0 MB 0 EA 0 EA
PatrickG 0 MB 0 MB 0 EA 0 EA
AlexisM 0 MB 0 MB 0 EA 0 EA
TheresaF 0 MB 0 MB 0 EA 0 EA
FrankE 0 MB 0 MB 0 EA 0 EA
RomeliaC 0 MB 0 MB 0 EA 0 EA
Local Groups Block limit Usage File limit Usage
nfsnobody 0 MB 0 MB 0 EA 0 EA
Sales 0 MB 0 MB 0 EA 0 EA
CustomerService 0 MB 0 MB 0 EA 0 EA
Exec 0 MB 0 MB 0 EA 0 EA
Tech 0 MB 0 MB 0 EA 0 EA
Purchasing 0 MB 0 MB 0 EA 0 EA
Shipping 0 MB 0 MB 0 EA 0 EA
Apply

Quota management allows the administrator to apply limitation on capacity and number of files used by each user.

1. Select logical volume to apply the quota value from SELECT LOGICAL VOLUME pull down menu.
2. Check the **ENABLE QUOTA** box and click **APPLY**. By clicking **APPLY**, additional settings will become visible.

3. Set the block limit (capacity limit) for all users/user groups by entering a value in the SET ALL BLOCK LIMITS field or Set a different block limit for each user/user group by entering values in the user/user group fields below.
4. Set the maximum number of files allowed for all users in the NUMBER OF FILES field or Set a different file limit for each user/user group by entering values in the user/user group fields below.
5. Click **APPLY** to complete.

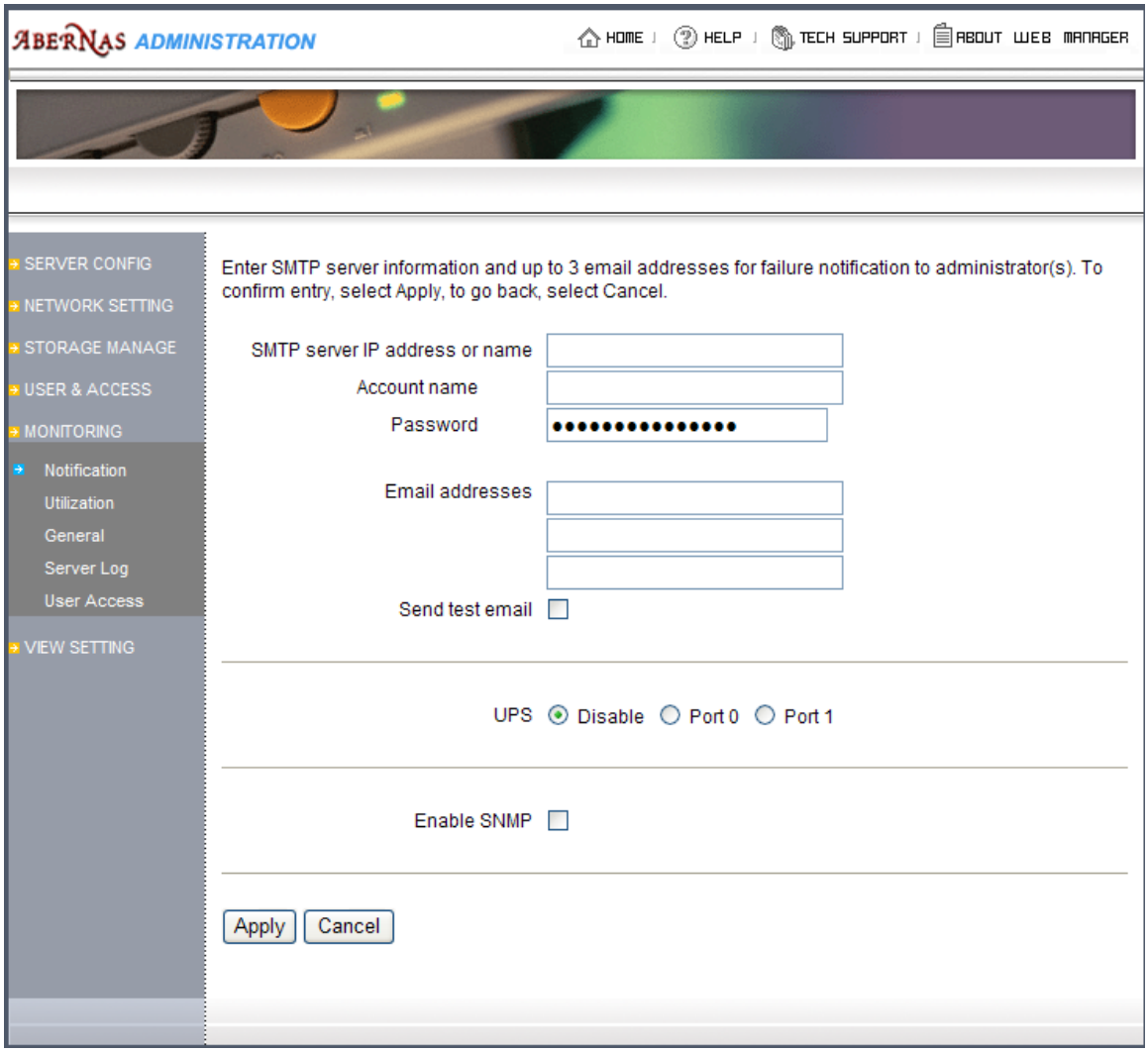
NOTE:

Usage field next to BLOCK LIMIT and FILE LIMIT shows the current usage by the user.
Quota scheme is designed to monitor aggregate usage of all the users/groups. As a result, sum of quota assigned for the logical volume may exceed the total capacity of the logical volume. Quota is not active if the logical volume has "EVERYBODY ACCESS" assigned for Access Control. Deleting logical volume when quota is assigned will erase all quota assignment. To reset quota, deactivate and reactivate quota for desired logical volume.

CAUTION:

When using in SFM configuration, enable quota before enabling SFM. If SFM requires disabling, disable quota before disabling SFM.

Web Administration Interface > MANAGE > Monitoring – Notification



The AberNAS is equipped with features that will notify designated administrators with failure notifications via e-mail.

Setup a Failure notifications Procedure:

1. SMTP Server IP Address – Enter the IP address and Account information of an outgoing mail server that will be used to send e-mail notifications.
2. E-mail Addresses – Enter the full e-mail addresses (e.g. name@company.com) for up to three administrators who are to be notified when any of the above selected failures occur.
3. Send Test E-mail – If selected, a test notification message will be sent to each e-mail address entered in the E-MAIL ADDRESSES fields after the APPLY button is pressed.
4. Enable UPS – The COM port of the ABERNAS may be connected to an Uninterruptable Power Supply (UPS) monitor port. When the UPS is activated due to a power loss, a notification will be sent to each e-mail entered in the E-MAIL ADDRESSES fields

.

NOTE:

Must use a simple signaling Cable for proper functionality with the AberNAS system.

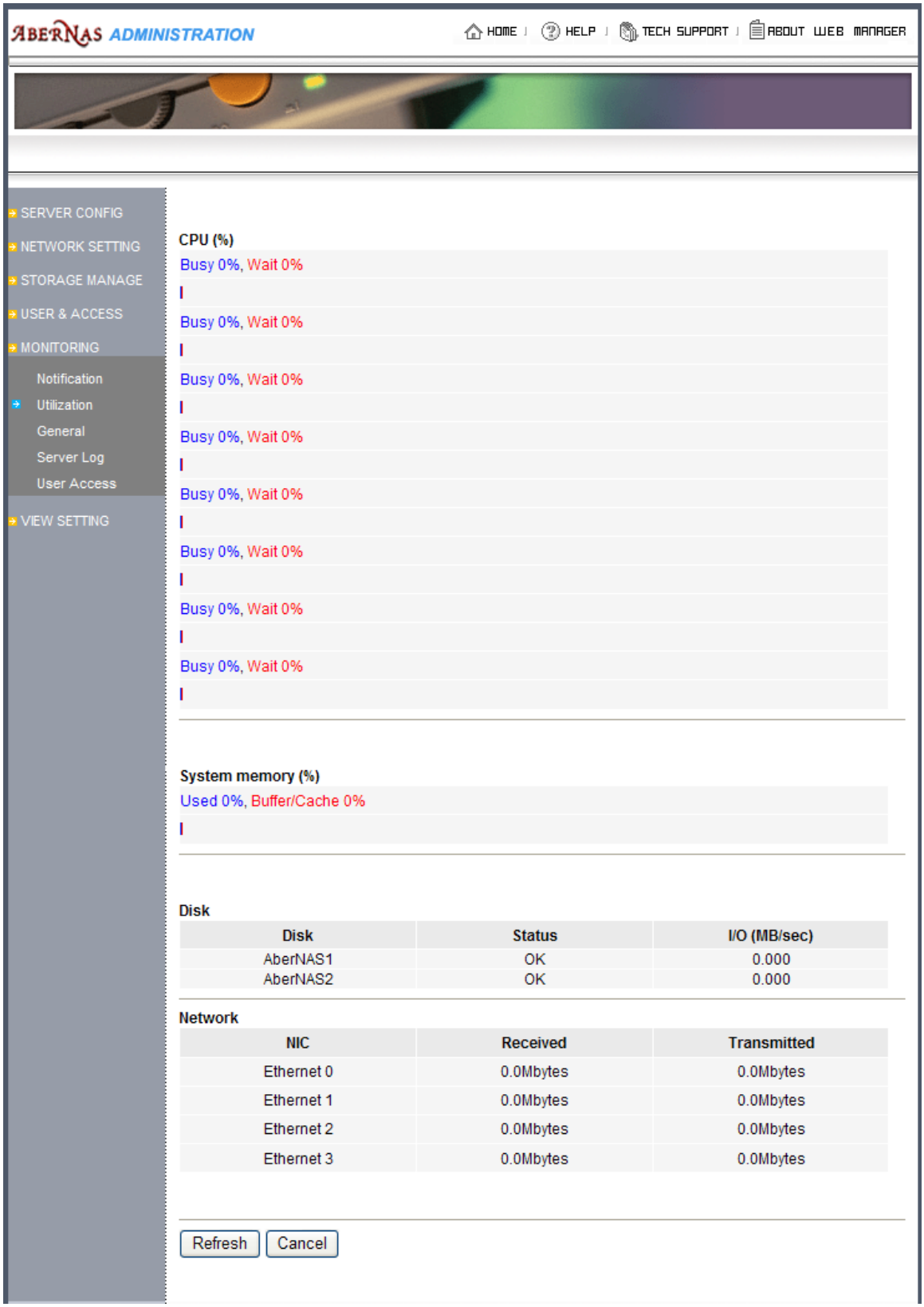
5. SNMP – When enabled, monitoring applications may receive ABERNAS status via SNMP protocol.
6. Temperature/Fan Monitoring – Temperature, CPU/Chassis fans may be monitored via Web administration. In addition, any over-temp. (above 75°C ambient) or fan failure (if connected fans have tachometer output for RPM) status will be notified by e-mail.

CAUTION:

By default, temperature and fan monitoring are disabled. This is to prevent automatic system shutdown when an unknown motherboard is configured. The AberNAS OS must be able to communicate with the server monitoring chips (often referred to lM or I2C sensors) in order to properly use this feature. Unrecognized chips may result in improper temperature and fan readers.

7. Click **APPLY** to complete, or click **CANCEL** to discard the changes and return to the Administration Home Page.

Web Administration Interface > MANAGE > Monitoring – Utilization



Monitor the following the AberNAS utilization parameters in real time:

CPU – Displays the percentage of CPU utilization. Multiple CPUs or CPU cores will be listed individually.

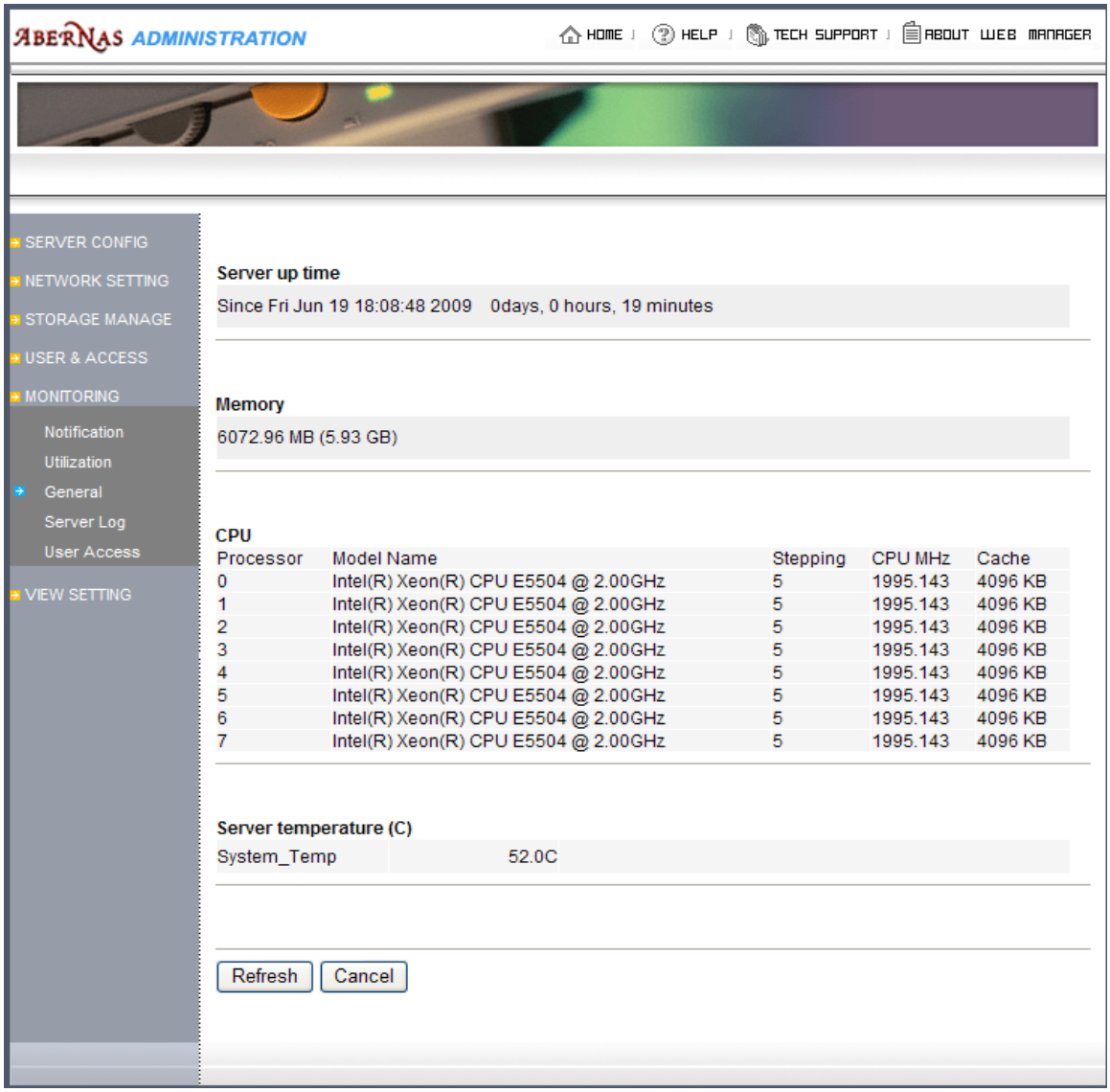
System Memory – Displays % of system memory being used and includes cached data.

Disk I/O Utilization – Displays disk I/O in MB.

Network Utilization – Displays accumulated received and transmitted to and from the ABERNAS. Click **REFRESH** to view the latest status, or Click **CANCEL** to return to the Administration Home Page.

NOTE:
Utilization page refreshes every 30 seconds.

Web Administration Interface > MANAGE > Monitoring – General


ABERNAS ADMINISTRATION
HOME | HELP | TECH SUPPORT | ABOUT WEB MANAGER
SERVER CONFIG
NETWORK SETTING
STORAGE MANAGE
USER & ACCESS
MONITORING
Notification
Utilization
General
Server Log
User Access
VIEW SETTING
Server up time
Since Fri Jun 19 18:08:48 2009 0days, 0 hours, 19 minutes
Memory
6072.96 MB (5.93 GB)
CPU
Processor Model Name Stepping CPU MHz Cache
0 Intel(R) Xeon(R) CPU E5504 @ 2.00GHz 5 1995.143 4096 KB
1 Intel(R) Xeon(R) CPU E5504 @ 2.00GHz 5 1995.143 4096 KB
2 Intel(R) Xeon(R) CPU E5504 @ 2.00GHz 5 1995.143 4096 KB
3 Intel(R) Xeon(R) CPU E5504 @ 2.00GHz 5 1995.143 4096 KB
4 Intel(R) Xeon(R) CPU E5504 @ 2.00GHz 5 1995.143 4096 KB
5 Intel(R) Xeon(R) CPU E5504 @ 2.00GHz 5 1995.143 4096 KB
6 Intel(R) Xeon(R) CPU E5504 @ 2.00GHz 5 1995.143 4096 KB
7 Intel(R) Xeon(R) CPU E5504 @ 2.00GHz 5 1995.143 4096 KB
Server temperature (C)
System_Temp 52.0C
Refresh
Cancel

Monitor the following areas real time:

Server Uptime – Displays how long the AberNAS has been running in days, hours and minutes since it was turned on.

Server Temperature – Displays the current temperature and fan status of the AberNAS.

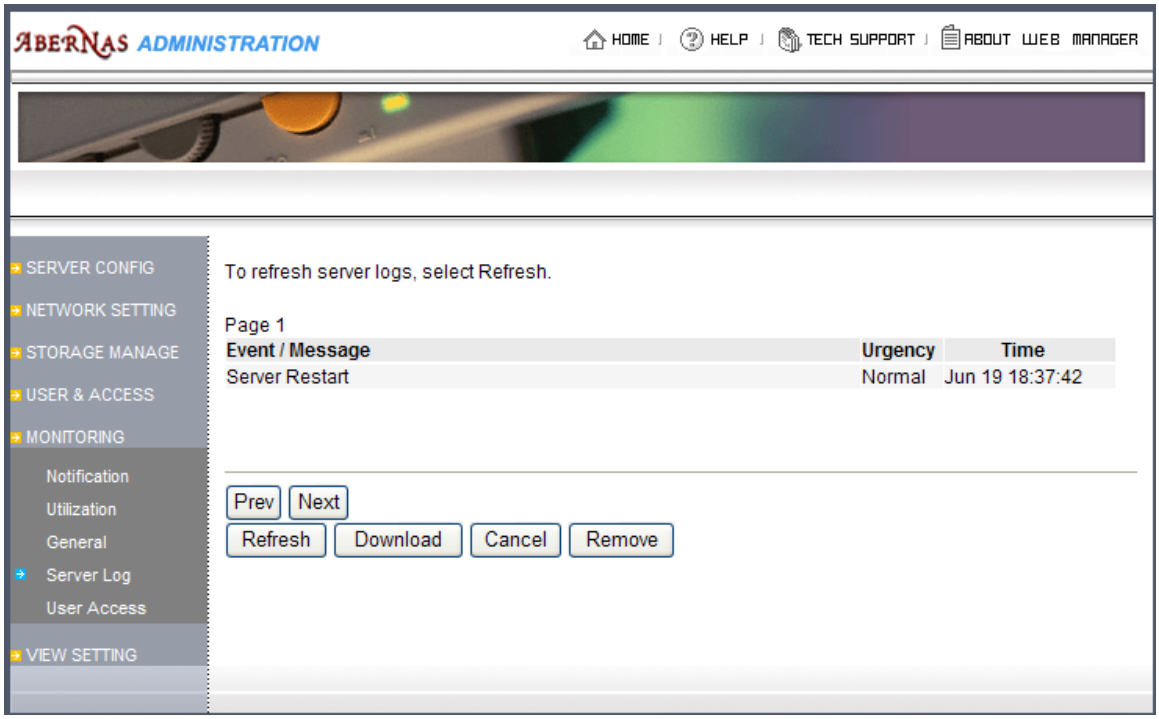
NOTE:

If the temperature reaches above 75°C, "Over-temp" is displayed and an e-mail notification is sent to the addresses listed on the Notification page.

Fan Status (RPM) – Displays rotation speed and status of the CPU and chassis fans in RPM.

SNMP – Displays "Enabled" if activated. To view the latest status, click **REFRESH**, or Click **CANCEL** to return to the Administration Home Page.

Web Administration Interface > MANAGE > Monitoring – Server Log



All actions, events and messages occurring on the AberNAS system are recorded and can be viewed on the **SERVER LOG** page of the Web Administration GUI. This comprehensive log of activities can be useful for troubleshooting problems or managing the AberNAS system.

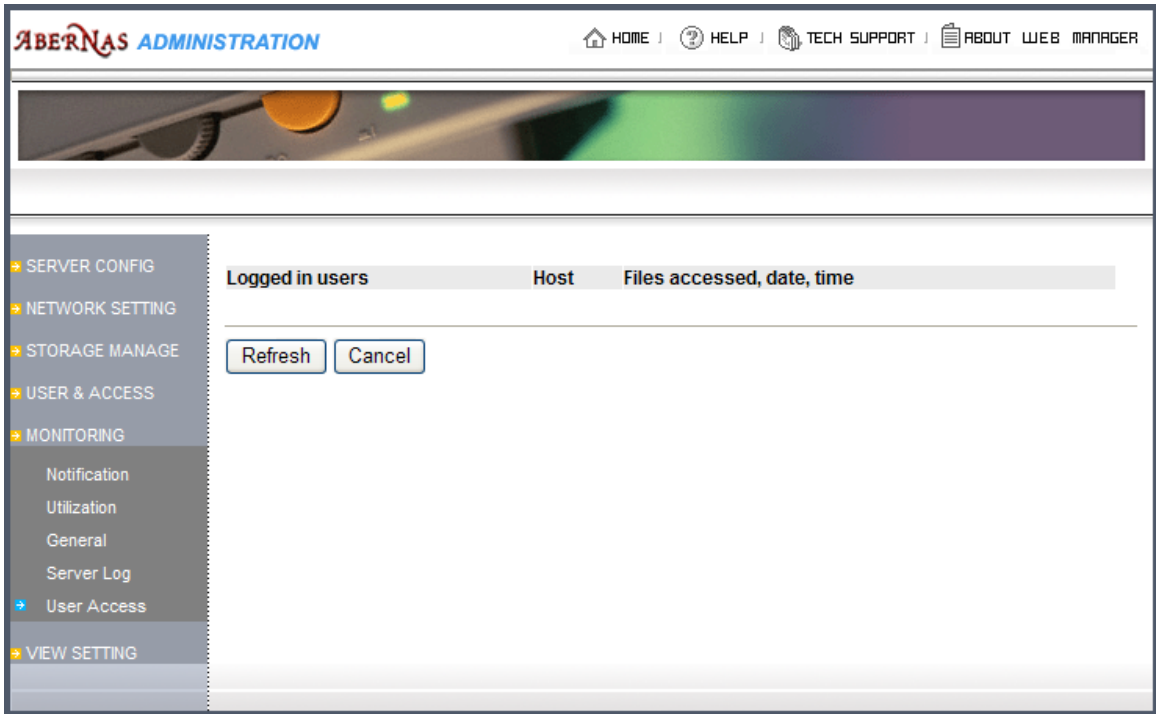
NOTE:

The AberNAS begins recording all server events and activities in the server log as soon as it is installed.

View A Log of Activities:

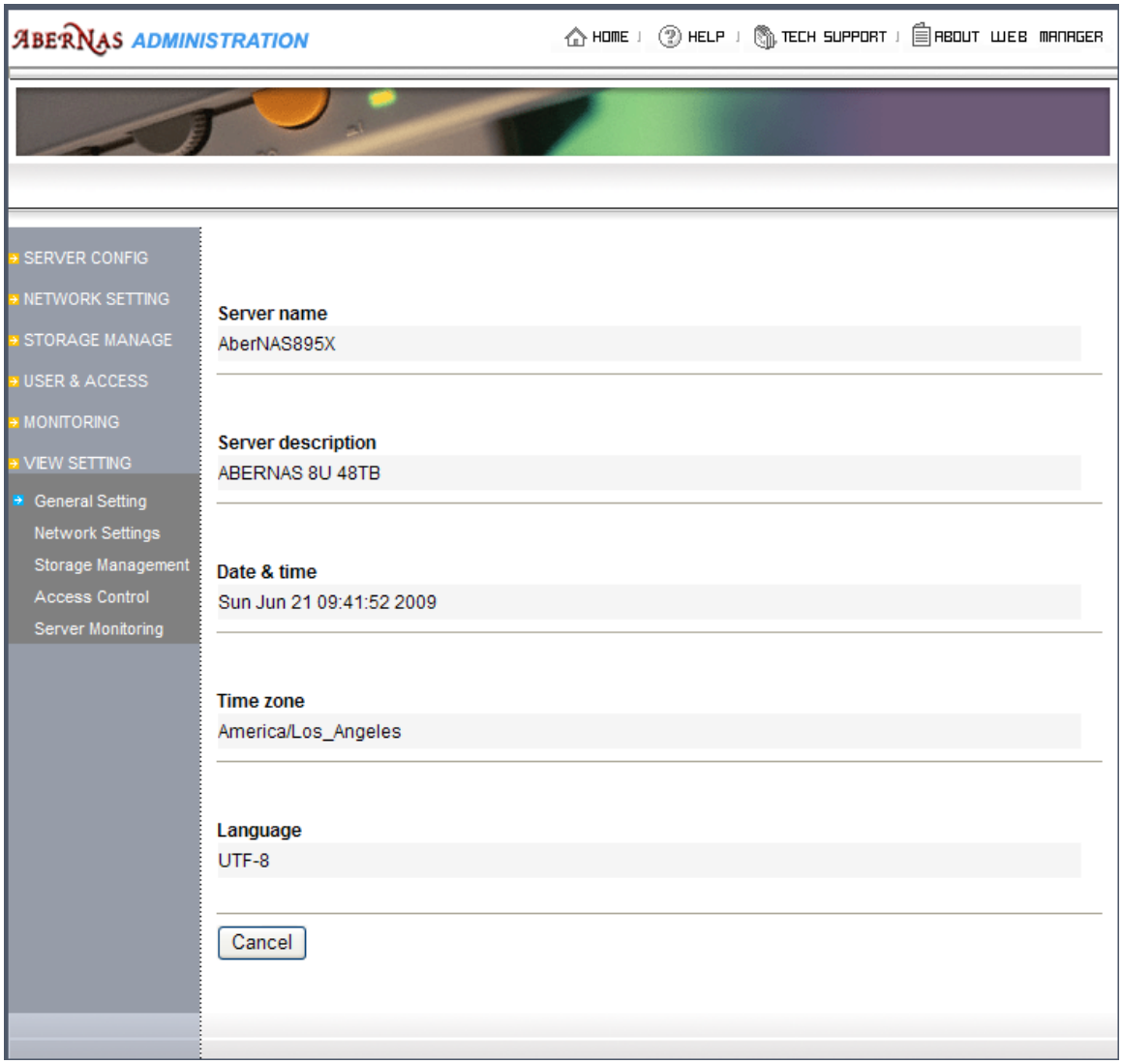
Navigate to the SERVER LOG page and enter the number of days to be displayed in the logs. Click REFRESH to view the most current logs. Click REMOVE to delete the current log information. Click CANCEL to return to the Administration Home Page. The server log on this page is filtered to report events that were determined to be most commonly used. For an expanded log of the ABERNAS, login via the command line. All directories in **/var/log/** can be viewed for various types of system logs.

Web Administration Interface > MANAGE > Monitoring – User Access



This feature allows the administrator to view information about the user(s) that are accessing the ABERNAS system, including the type of computer(s) used to log in and details about the file(s) it accessed. Click **REFRESH** to update the list of user(s) and the file(s) currently being accessed, or Click **CLOSE** to return to the Administration Home Page.

Web Administration Interface > MANAGE > View Setting – General Setting



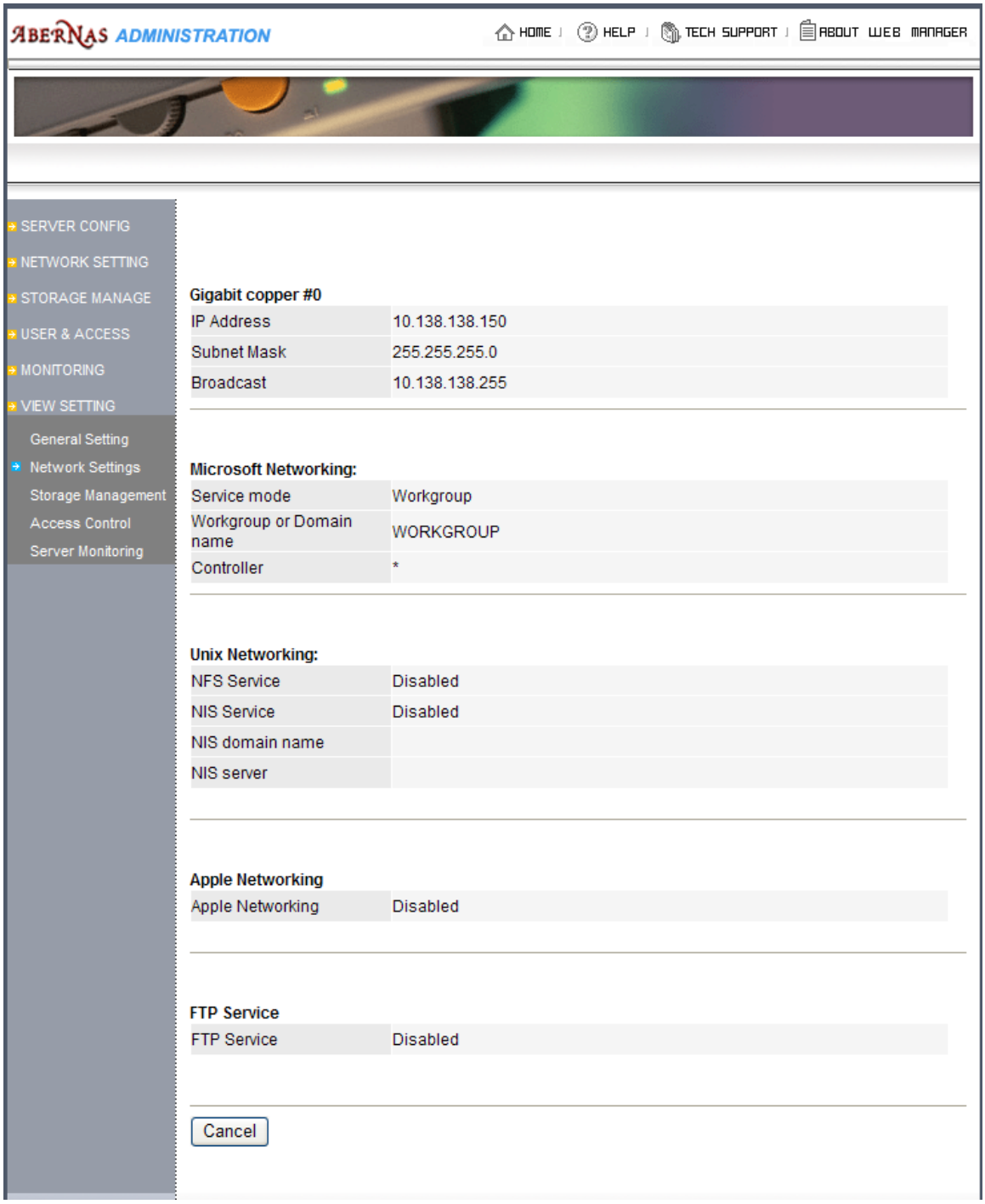
View the Server Configuration settings for the following:

- Server Name
- Server Description
- Date and Time
- Time Zone
- Language
- NTP

These settings can be changed on the SERVER CONFIGURATION pages of the ABERNAS Web Administration GUI.

Click **CANCEL** to return to the Administration Home Page.

Web Administration Interface > MANAGE > View Setting – Network Settings



View the Network Setting configurations for the following:

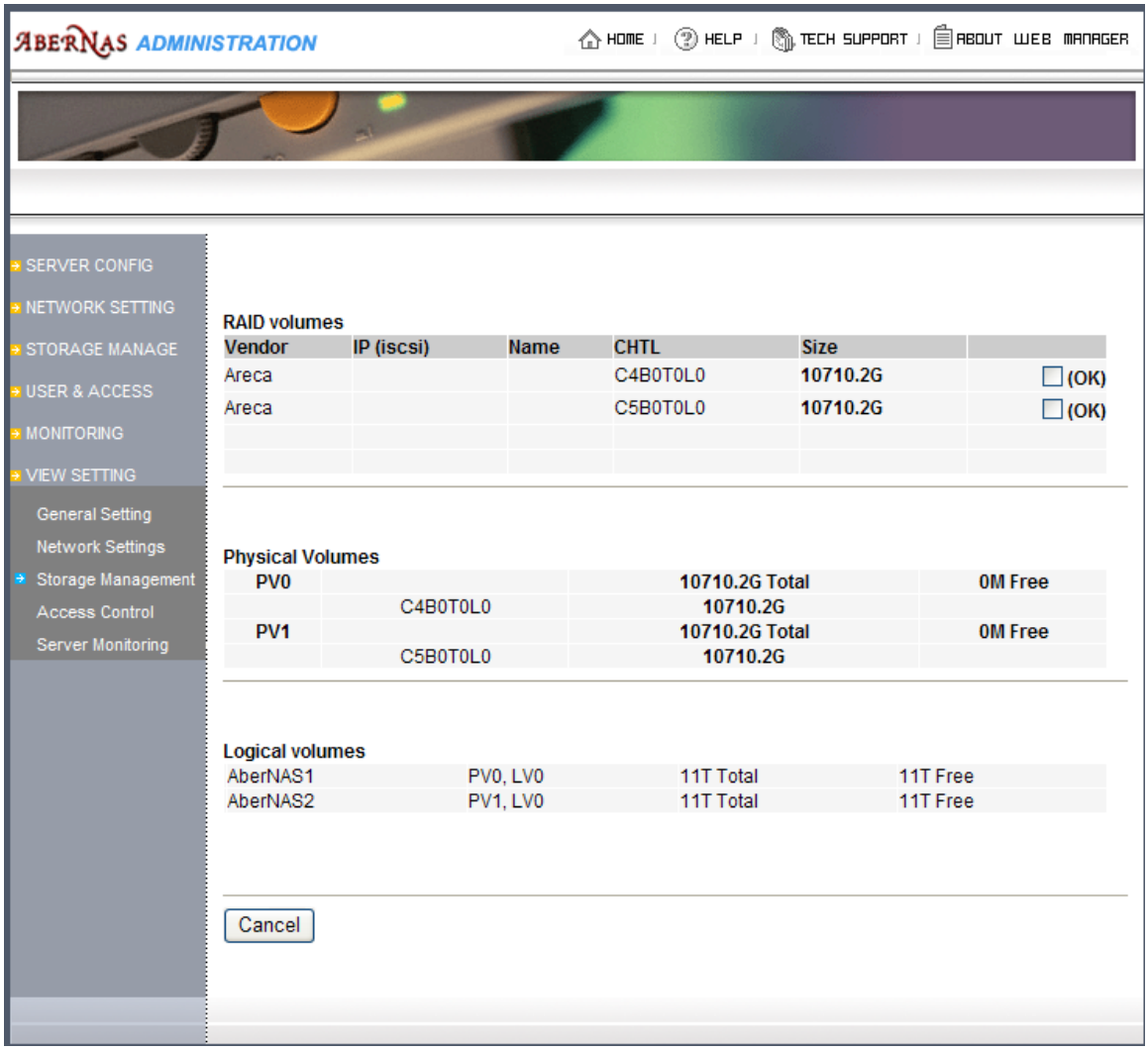
- TCP/IP settings for Gigabit
- Port Bonding
- Microsoft Networking
- UNIX Networking

- Apple Networking
- LDAP Client
- DHCP Service
- FTP Service
- iSCSI Initiator Service

These settings are configured and can be changed on the NETWORK SETTINGS pages of the ABERNAS Web Administration GUI.

Click **CANCEL** to return to the Administration Home Page.

Web Administration Interface > MANAGE > View Setting – Storage Management



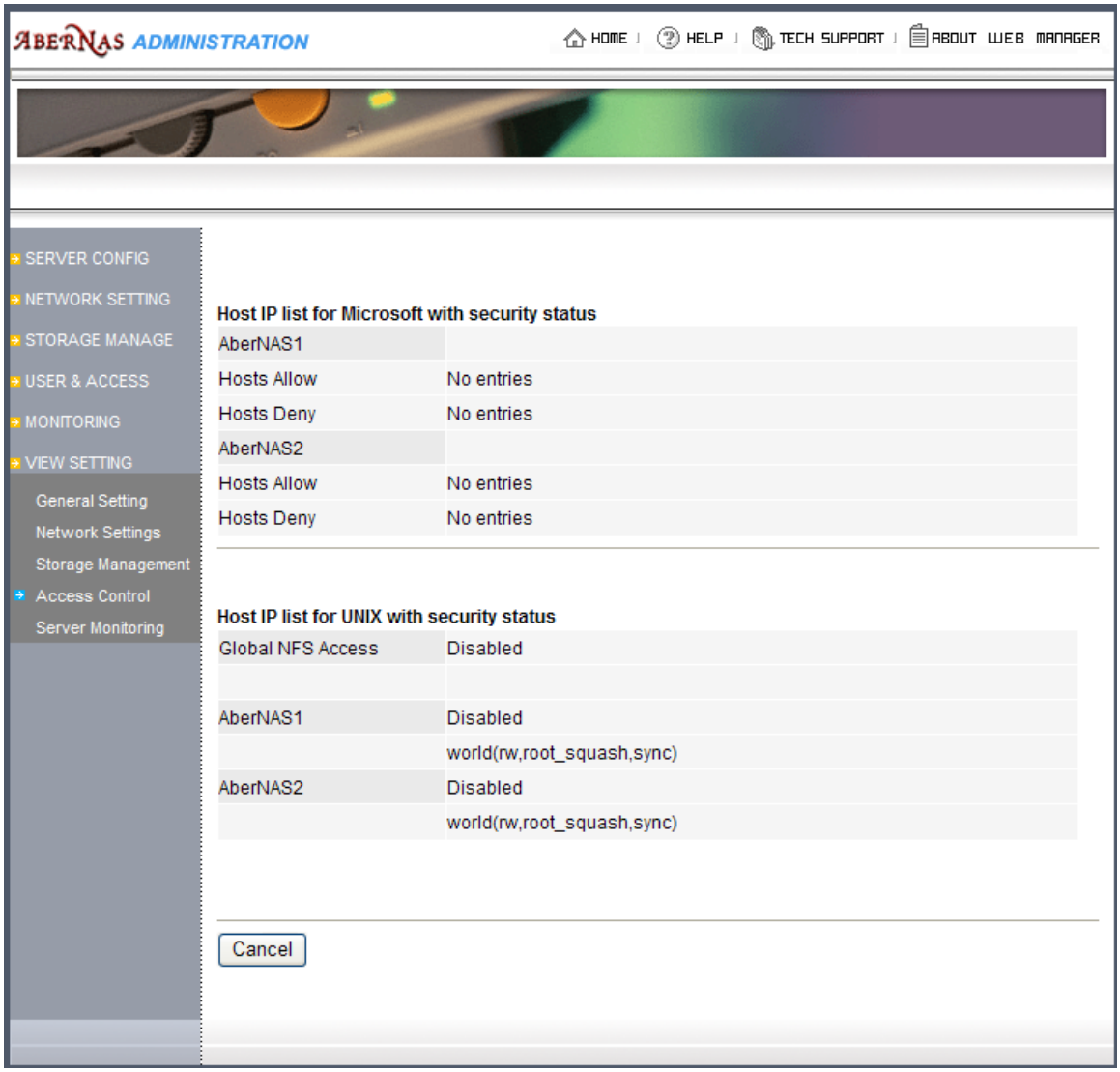
View the Storage Management configurations for the following:

- RAID Volumes
- Physical Volumes
- Logical Volume Shares
- File System
- Maintenance

These settings are configured and can be changed on the SERVER MANAGEMENT pages of the AberNAS Web Administration GUI.

Click **CANCEL** to return to the Administration Home Page.

Web Administration Interface > MANAGE > View Setting – Access Control



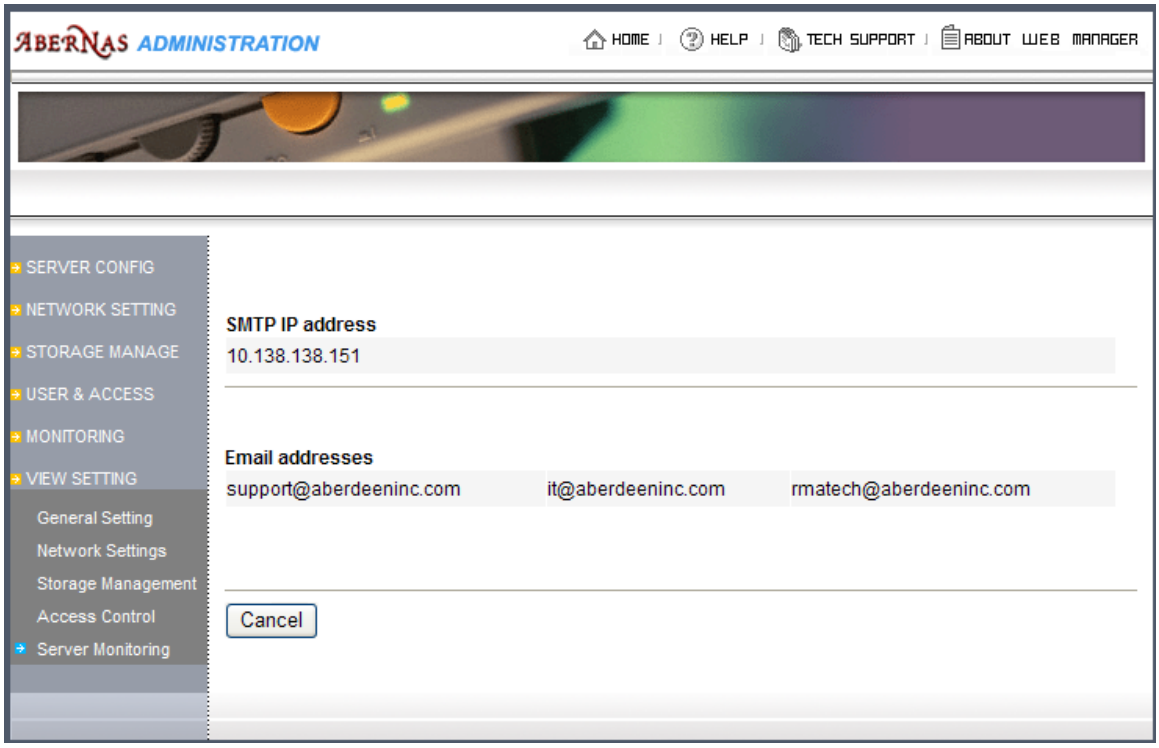
View the User & Access configurations for the following:

- IP address list of all Microsoft hosts with security status
- IP address list of all UNIX hosts with security status

These settings are configured and can be changed on the USER & ACCESS pages of the AberNAS Web Administration GUI.

Click **CANCEL** to return to the Administration Home Page.

Web Administration Interface > MANAGE > View Setting – Server Monitoring



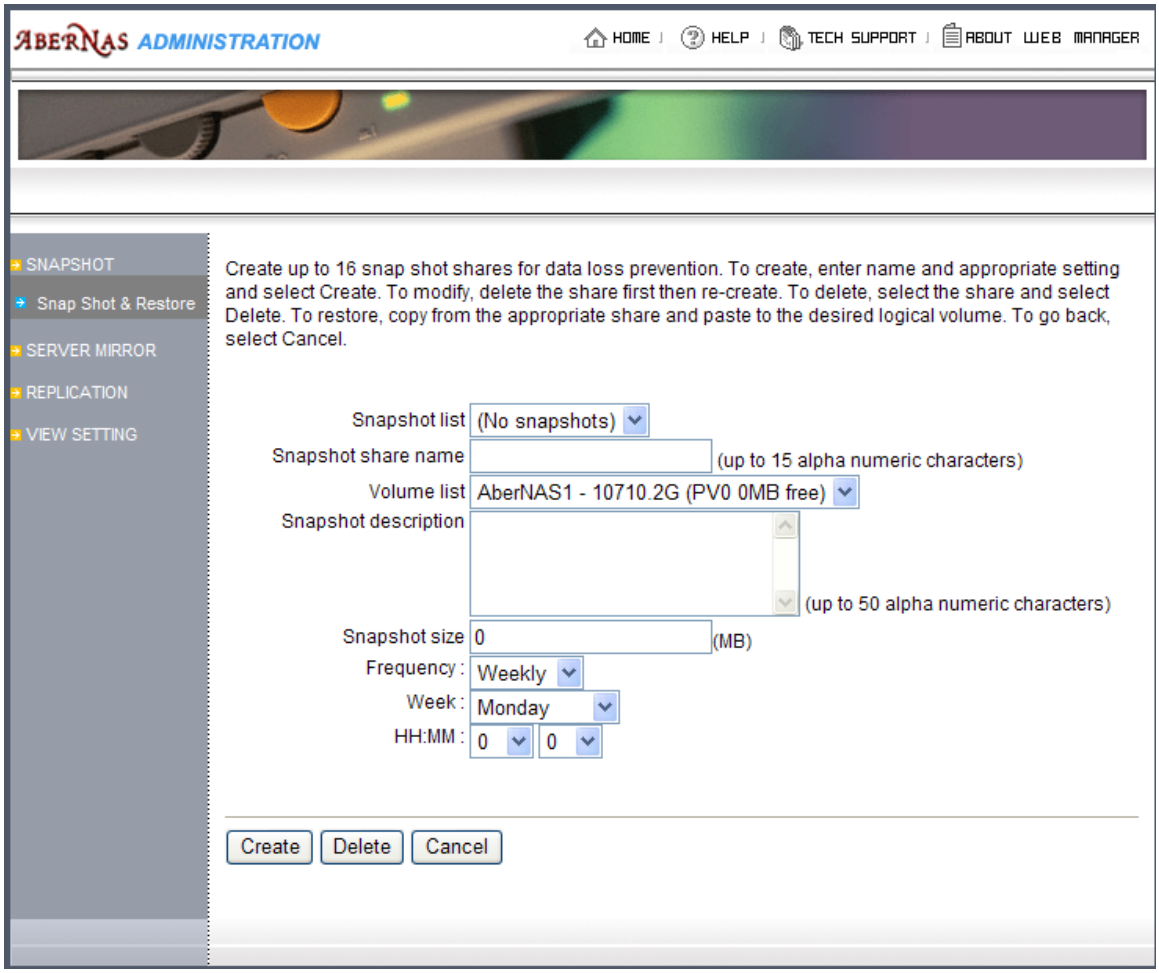
View the Server Monitoring configurations for the following:

- SMTP IP address
- Email Addresses (up to three notification email addresses)

These settings are configured and can be changed on the SERVER MONITORING NOTIFICATIONS pages of the ABERNAS Web Administration GUI.

Click **CANCEL** to return to the Administration Home Page.

Web Administration Interface > Backup Mirror and Restore > Snapshot



Snapshot and Restore:

The AberNAS is equipped with Snapshot technology where it can take scheduled “snapshot” of its Logical Volume(s) to retrieve files that were accidentally erased. The total number of Snapshots per AberNAS system is three, regardless of number of PV’s or LV’s existent on the system. The three volume limit was placed as it is the typical maximum used by users. The quantity of Snapshot volumes may be increased if necessary, please contact Aberdeen Technical support for details.

NOTE:

Snapshots are assigned to individual logical volumes as snapshot volumes. Snapshot volumes reside in the same physical volume as the logical volume. As a result, physical volumes must have adequate free space to support both the snapshot volume and contents of the logical volumes. The size of the snapshot volume varies depending on the environment in which the AberNAS system is deployed. If there are frequent changes to the files by large number of users, and multiple snapshots are required per logical Volume, then, higher capacity should be considered for the snapshot volume. The AberNAS uses block level method, where changes in the logical volume are written to the snapshot volume(s) simultaneously. As a result, having multiple snapshot volumes per logical volume requires multiple writes. Performance degradation for disk I/O is affected by the number of snapshot volumes per logical volume and the frequency of changes in the logical volume. If the maximum capacity for the snapshot volumes has been reached, the system will no longer be able to create new snapshots. When this occurs, the administrator will be notified.

Create Snapshots:

1. Input name in the SNAPSHOT SHARE NAME field (Up to 15 alpha numeric characters).
2. Select the LV from the VOLUME LIST pull down menu.

NOTE:
The PV in which this LV will reside must have adequate free space.

3. Input description in the SNAPSHOT DESCRIPTION field. This is optional.
4. Enter the capacity (in MBs) for Snapshot Volume in the SNAPSHOT SIZE field. (Time based is the specified time that each Snapshot is taken. For example, hour of the day, day of the week, or date of the month.
5. For Time based schedule, select DAY, WEEK or MONTH from the FREQUENCY pull down menu :

- Day: Enter hour and minute of the day to take Snapshot. Value of 1 is 1:00AM.
- Week: Enter day, hour and minute of the week to take Snapshot. Value 1 is Monday.
- Month: Enter date, hour and minute of the month to take Snapshot. Value of 1 is 1st.

6. Click **CREATE** to create Snapshot Volume, or Click **CANCEL** to return to the Administration Home Page.

Delete Snapshot:

1. Select desired Snapshot from the SNAPSHOT list. If you cannot locate the Snapshot Volume, change to another LV by selecting a different LV from VOLUME LIST pull down menu. Click **DELETE** to delete the Snapshot Volume, or click **CANCEL** to return to the Administration Home Page.

Modify Snapshot:

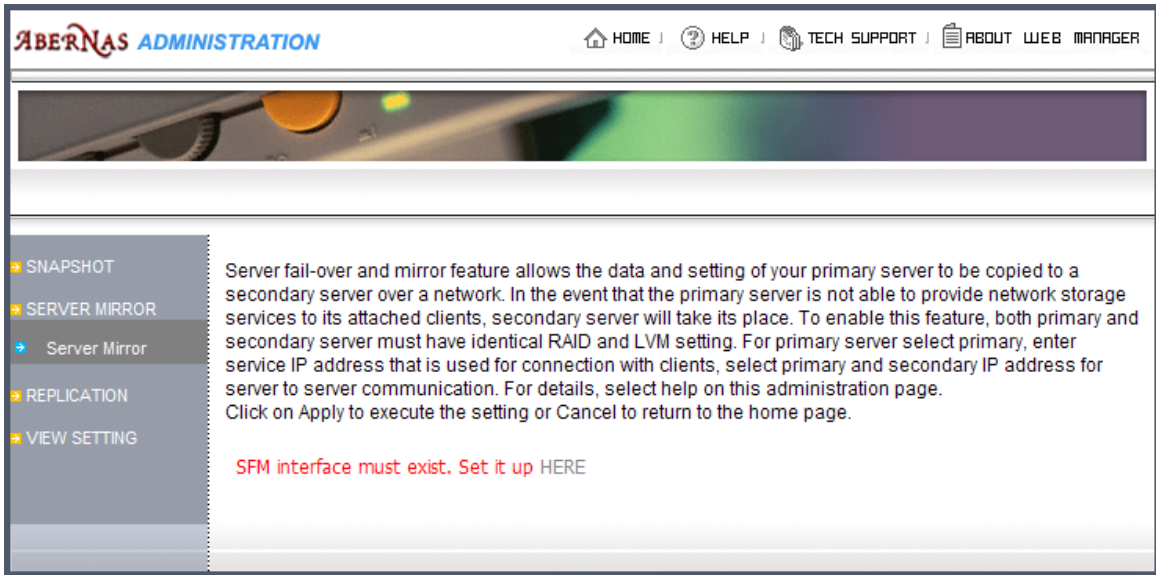
First delete the Snapshot, then recreate. See above for instructions for creating and deleting Snapshots. Click **CANCEL** to undo changes and return to home page.

Backup Software Agent Install:

The Backup Utility on the AberNAS has been removed. Instead, RPM package manager was included in the AberNAS embedded OS. As a result, users can now install backup agents from various backup software packages available on the market. Some of the backup software supported by the AberNAS are listed below. In most cases, the AberNAS can be configured to support backup software that is not part of the below list. Please contact Aberdeen Technical Support for updates or consultation to add your software to the list.

1. Veritas Backup Exec
2. Veritas Net Backup
3. Amanda
4. BRU Backup Software
5. Legato Networker

Web Administration Interface > Backup Mirror and Restore > Server Mirror


ABERNAS ADMINISTRATION
HOME
HELP
TECH SUPPORT
ABOUT WEB MANAGER
SNAPSHOT
SERVER MIRROR
Server Mirror
REPLICATION
VIEW SETTING
Server fail-over and mirror feature allows the data and setting of your primary server to be copied to a secondary server over a network. In the event that the primary server is not able to provide network storage services to its attached clients, secondary server will take its place. To enable this feature, both primary and secondary server must have identical RAID and LVM setting. For primary server select primary, enter service IP address that is used for connection with clients, select primary and secondary IP address for server to server communication. For details, select help on this administration page.
Click on Apply to execute the setting or Cancel to return to the home page.
SFM interface must exist. Set it up HERE

Server Fail-over and Mirror:

Server Fail-over and Mirror (SFM) is an optional feature used to bind two AberNAS servers as one so as to write data to both systems simultaneously. In addition, this feature also provides server service fail-over so that clients attached to the primary server can be serviced by the secondary server in the event that primary server is not able to provide the service. The clients accessing the primary server, in most cases, will not notice the fail-over process when the secondary AberNAS takes over. Each AberNAS system has two groups of network port(s). One group is dedicated for client serving (Data ports) and the other group is dedicated for data copying and communicating (SFM ports) with each other. Both groups of network ports may be bonded for higher throughput as well as fail-over within NIC ports.

Before Configuring SFM:

- Both systems should have at least one NIC port dedicated for SFM use. Connection between two systems may be via crossover cable or connected to a switch. When using a switch, it is recommended that the switch for the SFM ports be separate from Data ports.

NOTE:

SFM port may be configured simply by clicking on the available port and selecting SFM. TCP/IP information is not needed for SFM port.

- Both systems must have same number of PVs and LVs as well as same capacity for PVs and LVs. Name the PVs and LVs the same for both systems.
- Both systems should be connected to the same subnet.
- If ADS/PDC and/or NIS synchronization is planned, synchronize ADS/PDC and/or NIS before starting SFM configuration for the primary server. If ADS/PDC and/or NIS synchronization need to be disabled, disable SFM first.
- Plan three IP addresses:

1. Data IP address for primary server. For example, 10.1.1.100
2. Data IP address for secondary server. For example, 10.1.1.101

3. IP address for Service port. Service port is the virtual port used for clients to connect to the AberNAS system in SFM mode. For example, 10.1.1.100.
4. For this manual, the following IP addresses will be used for example:

- Primary server IP address: 10.1.1.100
- Secondary server IP address: 10.1.1.101
- Service port IP address: 10.1.1.200

Configure SFM:

1. Power up primary server. Secondary server must be turned off.
2. Configure the TCPI/IP for Data port and SFM port in Network Setting TCP/IP configuration. IP address for primary server's Data port would be (10.1.1.100). SFM port is assigned by the AberNAS, simply click on the available NIC port, SFM radio button and click **Apply**.
3. Go to SFM page found in Backup, Mirror and Restore section, and select Primary radio button. Input Service IP address (10.1.1.200) and Secondary IP address (10.1.1.101)
4. Reboot the primary server. Configuration of the primary server is done.
5. Power up secondary server. Primary server should be on at this time
6. Configure the TCP/IP for Data port and SFM port in Network Setting / TCP/IP configuration. The IP address for secondary server's Data port would be (10.1.1.101). The SFM port is assigned by the AberNAS. Simply click on the available NIC port, SFM radio button and click **Apply**.
7. Go to SFM page found in Backup, Mirror and Restore section, and select Secondary radio button. Input Service IP address (10.1.1.200) and Primary IP address (10.1.1.100).
8. Reboot the secondary server.
9. Both systems' SFM page will now indicate that the sync is configured.
10. Clients need to map to network storage available from 10.1.1.200.
11. If the primary server should be incapable of serving its clients due to:

- Disconnected NIC port
- Power outage
- RAID volume corruption
- OS kernel panic

Secondary server will take over the service and all data on the primary server will be available, except, for those that were being written when the primary server failed.

Re-deploy Failed Primary Server:

1. Fix the problem that disabled the primary server.

NOTE:

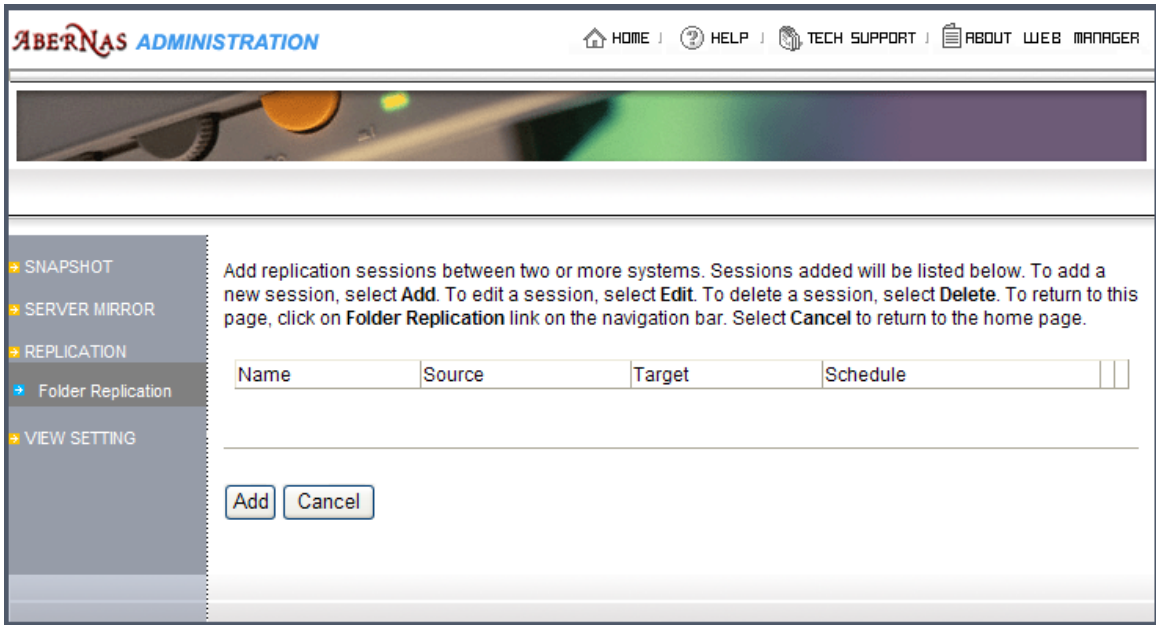
The re-deployment option of the primary server exists so that it can become the secondary server. The former secondary server now becomes the primary server.

2. The AberNAS server to be re-deployed must meet the requirements detailed under "**Before Configuring SFM"**.
3. Configure TCP/IP for the Data port in line with above example. Data port IP address would be (10.1.1.100).
4. If the server requires reconfiguration for RAID, Mirror the secondary server that is active.
5. Follow the steps above to configure the server to synchronize with primary server (formerly the secondary server).
6. Boot the former primary sever, it will sync and take position of secondary server.

NOTE:

• If the primary server had data stored before configuring SFM, it will immediately start to copy its data to the secondary server. Copy process time will vary depending on the size and type of file(s) on the primary server. When the former primary server (now secondary server) is re-deployed, data copy from former secondary server (now primary server) to former primary server (now secondary server) will take place immediately. Since server-to-server data mirroring involves multiple writes of same data, overall throughput of the AberNAS will be reduced. Performance varies on usage, type of data being transmitted, and the overall load on the AberNAS.

Web Administration Interface > Backup Mirror and Restore > Folder Replication


ABERNAS ADMINISTRATION
HOME
HELP
TECH SUPPORT
ABOUT WEB MANAGER
SNAPSHOT
SERVER MIRROR
REPLICATION
Folder Replication
VIEW SETTING
Add replication sessions between two or more systems. Sessions added will be listed below. To add a new session, select Add. To edit a session, select Edit. To delete a session, select Delete. To return to this page, click on Folder Replication link on the navigation bar. Select Cancel to return to the home page.
Name
Source
Target
Schedule
Add
Cancel

Folder Replication:

Add A Folder For Replication:

1. Click **ADD**. This page will expand to reveal more options.

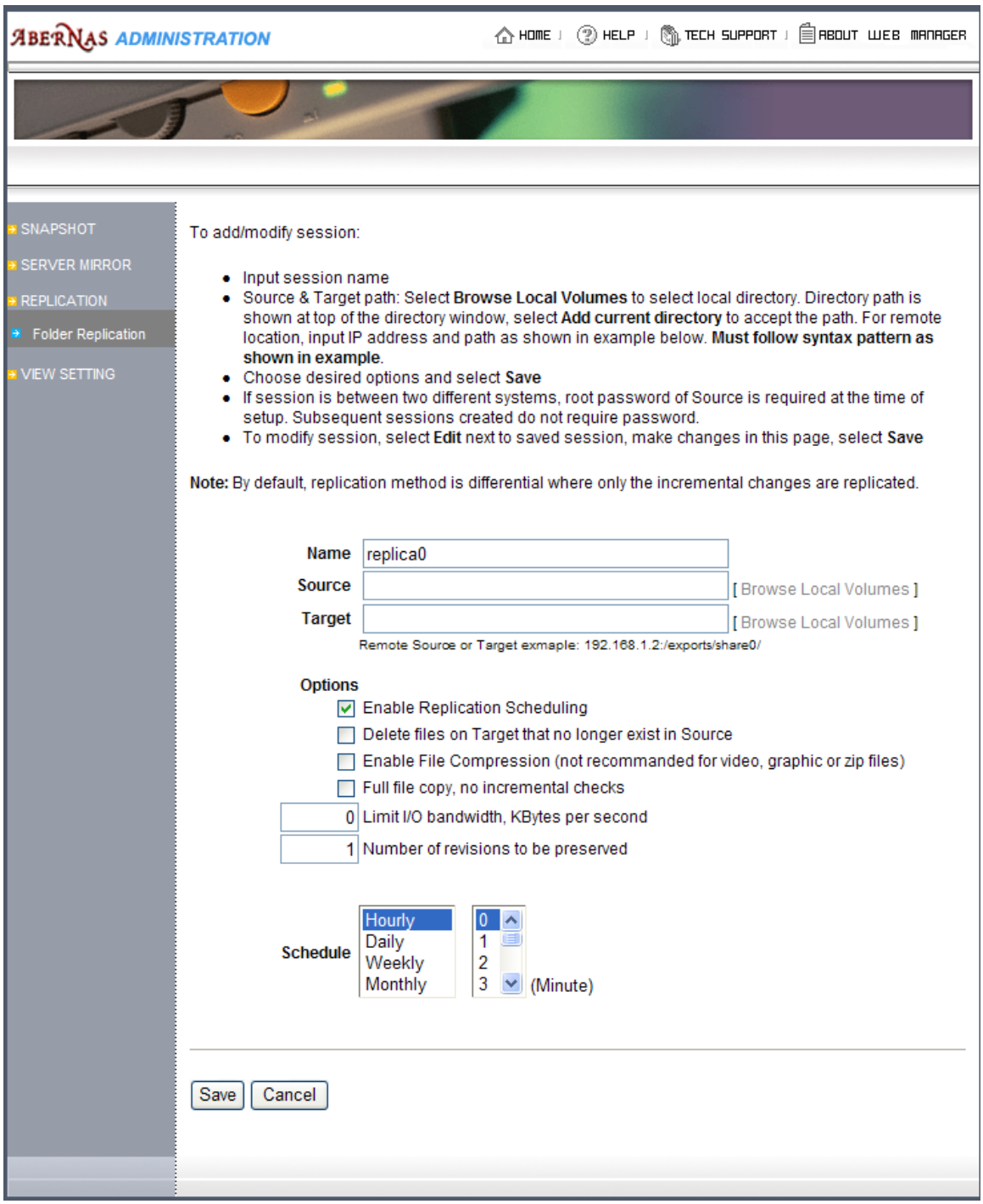
NOTE:
Folder replication can be configured with multiple schedules to support one to many and many to one.

2. Enter a unique name for the for this folder replication set (Up to 15 alpha numeric characters) in the NAME field.
3. Enter the full path to the source folder in the SOURCE field. Input the path for the target folder. For local folder path, click **BROWSE LOCAL VOLUMES**.

NOTE:
This is an example of how the path to the source should appear in the target field:
192.168.1.2:/exports/shared

4. Enter the full path of the location of the replicated folder, or target folder, in the TARGET field. To search for an existing folder, click **BROWSE LOCAL VOLUMES**.

NOTE:
This is an example of how the path to the source should appear in the source field:
192.168.1.2:/exports/shared


ABERNAS ADMINISTRATION
HOME | HELP | TECH SUPPORT | ABOUT WEB MANAGER
SNAPSHOT
SERVER MIRROR
REPLICATION
Folder Replication
VIEW SETTING
To add/modify session:
Input session name
Source & Target path: Select Browse Local Volumes to select local directory. Directory path is shown at top of the directory window, select Add current directory to accept the path. For remote location, input IP address and path as shown in example below. Must follow syntax pattern as shown in example.
Choose desired options and select Save
If session is between two different systems, root password of Source is required at the time of setup. Subsequent sessions created do not require password.
To modify session, select Edit next to saved session, make changes in this page, select Save
Note: By default, replication method is differential where only the incremental changes are replicated.
Name
replica0
Source
[Browse Local Volumes]
Target
[Browse Local Volumes]
Remote Source or Target exmaple: 192.168.1.2:/exports/share0/
Options
Enable Replication Scheduling
Delete files on Target that no longer exist in Source
Enable File Compression (not recommanded for video, graphic or zip files)
Full file copy, no incremental checks
0
Limit I/O bandwidth, KBytes per second
1
Number of revisions to be preserved
Schedule
Hourly
Daily
Weekly
Monthly
0
1
2
3
(Minute)
Save
Cancel

5. Set optional features for this Folder Replication set in the OPTIONS check boxes and fields.

Enable Replication Scheduling - Allows the schedule to be set for the replication. Schedule can be set in the Schedule section:

Hourly – Select minute of the hour.

Daily - Select the hour and minute of the day.

Weekly - Select the day, hour and minute of the week.

Monthly – Select date, hour and minute for the date of the month

Delete files on destination that no longer exists on source – As data is being copied to the target folder, it will delete any files that are no longer present in the source folder.

Enable file Compression – This feature compresses the file by utilizing the gzip compression protocol.

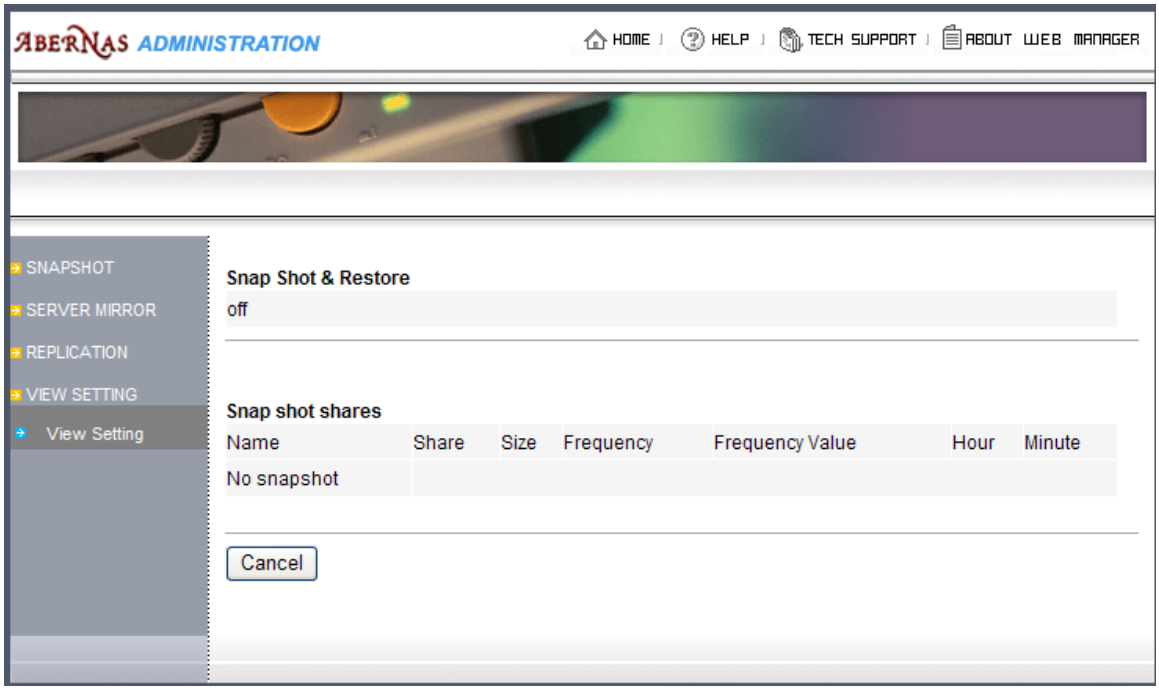
Full file copy – Default setting for folder replication is to copy only the changes (incremental checks) after the first full copy. This feature ignores the incremental checks and applies full copy.

Limit I/O bandwidth – Limits the amount of bandwidth allow for this Folder Replication set to the designated value in KBytes/second. A value of zero (0) will give this set unlimited bandwidth.

Number of revisions to be preserved – Indicates number of copy revisions to keep.

6. Set the **SCHEDULE** for replication by hours and minutes. Click **SAVE** to save this setting, or Repeat the process above to create multiple replication schedules or click **CANCEL** to return to the Administration Home Page.

Web Administration Interface > Backup Mirror and Restore > View Setting



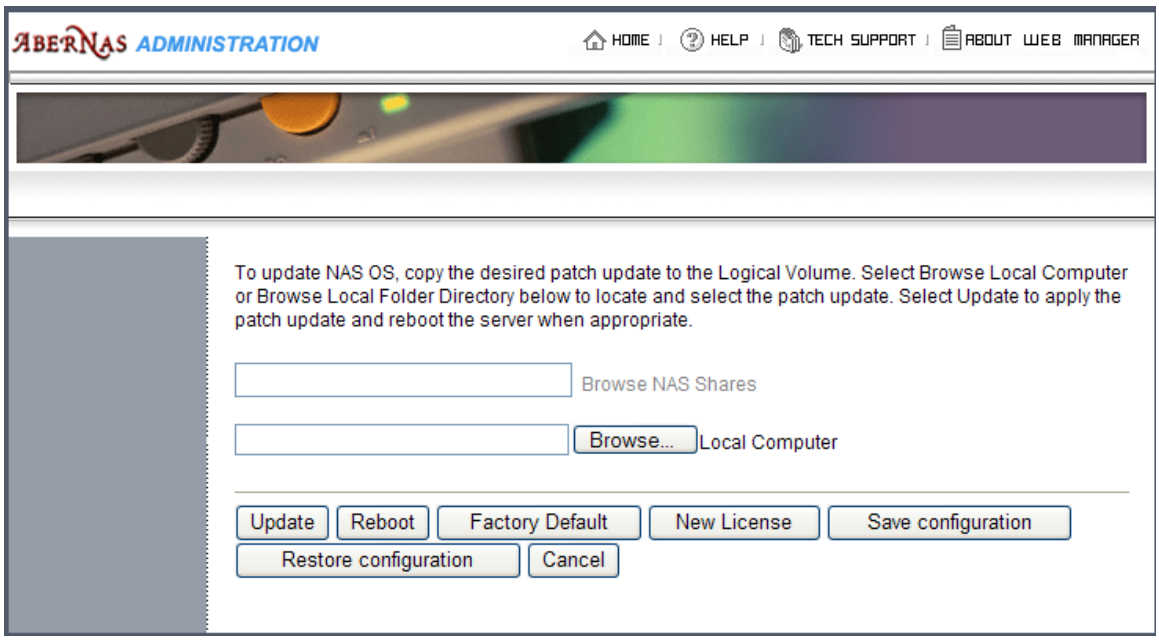
View Settings: Snap Shot and Restore

View the Snapshot & Restore configurations for the following:

Snapshot & Restore - Indicates whether the feature is on or off.
Snapshot Volumes - Displays all snapshot volumes available for snapshot and restore.

These settings are configured and can be changed on the SNAPSHOT & RESTORE page of the ABERNAS Web Administration GUI. Click **CANCEL** to return to the Administration Home Page.

Web Administration Interface > UPDATE –


ABERNAS ADMINISTRATION
HOME
HELP
TECH SUPPORT
ABOUT WEB MANAGER
To update NAS OS, copy the desired patch update to the Logical Volume. Select Browse Local Computer or Browse Local Folder Directory below to locate and select the patch update. Select Update to apply the patch update and reboot the server when appropriate.
Browse NAS Shares
Browse...
Local Computer
Update
Reboot
Factory Default
New License
Save configuration
Restore configuration
Cancel

AberNAS Update:

Software updates for the AberNAS will be available from time to time. Contact Aberdeen Technical Support to check if updates are available and to obtain download information.

CAUTION:

Be sure to update your AberNAS when it is not in service. A Reboot will be required and will temporarily disable the service that the AberNAS provides to its users. Updates should be treated like system BIOS updates. If you are not experiencing any problems, do not perform any updates.

Updating the AberNAS To The Latest Patch:

1. Login to the Web Administration GUI of the AberNAS and proceed to the **UPDATE** section.
2. Click **BROWSE** and locate the patch file.
3. Select the patch file. (The path to the file will be displayed in the text field).
4. Click **UPDATE** to complete this process or click **CANCEL** to cancel the update return to the Administration Home Page.
5. When prompted, click REBOOT to reboot the AberNAS system.

NOTE:

A Reboot will end services to any attached clients. Reboot only when appropriate.

CAUTION:

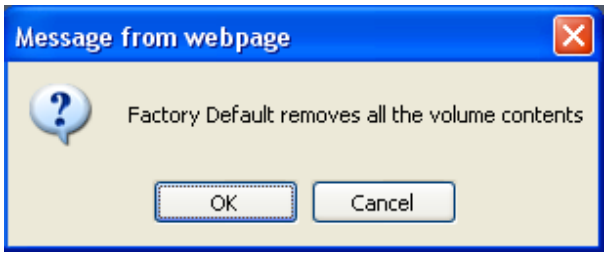
The AberNAS does not provide any warranty of data loss due to patch updates. It is recommended that users backup important data before updating patches for the OS. Applying an older version of the patch will revert the OS version to the previous version.

Reset the Server Settings Back to the Factory defaults:

Click **FACTORY DEFAULT** or click **CANCEL** to cancel the update return to the Administration Home Page.

CAUTION:

Selecting this option is destructive and will reset all settings, including deleting logical volumes (that will erase all data). The decision must be confirmed in the following confirmation window.



New License:

Click **NEW LICENCE** to enter the MAC address of a new port or other new options or click your browser's back button to cancel the update return to the Administration Home.